

УНИВЕРЗИТЕТ СИНГИДУНУМ

Департман за последипломске студије

САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

МАСТЕР СТУДИЈСКИ ПРОГРАМ

мастер рад

ДИГИТАЛНА ФОРЕНЗИКА И „СУВЕР“ КРИМИНАЛ

Ментор:

Гојко Грубор

Студент:

Игор Перић

Бр. индекса:

410288/2012

Београд

Јул 2013.

Апстракт

Рачунари су од тренутка појављивања постали део наше свакодневице. Данас се живот без рачунара не може замислити, што у послу, што у приватном животу. Познато је да се са развојом технологије развија и криминал. Од када су се рачунари, интернет и многи други мобилни уређаји појавили, број превара, проневера, крађа идентитета и разних злочина повезаних са порнографијом је у великој мери порастао. Дигитални докази су разни видови трагова злочина који се налазе на рачунару и око њега. Све се више развијају разни алати и програми за прикупљање ове посебне врсте доказа. Поред отисака и разних физичких трагова прикупљају се и дигитални трагови који се не могу прикупљати на класичан начин већ се мора прибећи посебном прикупљању доказа и њиховој детаљној анализи. Електронски доказ има све већи значај и због тога се са њима мора поступати врло пажљиво.

Форензика мобилних уређаја је врло значајна грана дигиталне форензике. Какав год да се уређај појави на тржишту мало ће времена проћи док га неко не злоупотреби. Зато је неопходно да се овој грани науке придаје све већа пажња, да би били и остали сигурни и да би наши паметни уређаји постали стварно "паметни", тако што ће бити способни да се заштите на прави начин.

Кључне речи: дигитална форензика, дигитални доказ, компјутерски криминал, мобилни уређаји, дигитално место злочина

Научна област: Информатика

Ужа научна област: Дигитална форензика

Abstract

Computers became part of our everyday life since the time of occurrence. Today we can not imagine life without computers, in business, as in personal life. It is known that with technology evolving and crime is evolving too. Since the computers, the Internet and many other mobile devices appeared, the number of fraud, embezzlement, identity theft and various crimes related to pornography has greatly increased. Digital evidence is different form of evidence of crimes that are on the computer and around. More and more various tools and programs are developed to collect these specific types of evidence. In addition to prints and various physical traces that are collected, digital traces are collected too, the clues that can not be collected in the traditional manner but must resort to a special gathering evidence and their detailed analysis. Electronic evidence is of increasing importance and therefore they must be dealt with very carefully.

Forensics of mobile devices is a very important branch of digital forensics. Whatever the device „hit“ the market, it don't tako much time untill someone abuses it. It is therefore essential that this branch of science is given more attention, and to make them safe and to keep our smart devices have become really "smart" so you will be able to protect themselves in the right way.

Keywords: flash, forensic, investigation, USB flash, flash memory, memory card

Scientific field: Computer Science

Specific sci-field: digital forensic

Садржај

Садржај слика, табела и графика	6
1. Методологија истраживачког пројекта	8
1.1. Уводне напомене и образложење рада	8
1.2. Предмет истраживања	10
1.3. Циљеви и задаци истраживања	10
1.4. Истраживачке хипотезе	11
1.5. Методе истраживања и ток истраживачког процеса	12
2. Порекло и корени дигиталне форензике	13
3. Основни појмови дигиталне форензике.....	16
4. <i>Cyber</i> криминал	21
5. Принцип дигиталне форензичке истраге.....	25
5.1. Прикупљање дигиталног доказа	25
5.2. Алати за прикупљање дигиталних доказа	26
6. Стање и напредак дигиталне форензике у Србији у борби против ИТ криминала	33
6.1. Високотехнолошки криминал у Србији	33
6.2. Дигитална форензика у Србији	36
7. Мобилни уређаји	37
7.1. Мобилни телефони.....	37
7.2. УСБ меморија	40
7.3. Меморијске картице	41
7.4. <i>PDA</i>	42
7.5. <i>MP3</i>	43
8. Заштита мобилних уређаја	44

8.1. Заштита мобилних телефона.....	44
8.2. Заштита флеш меморије	47
9. Дигитална форензика у функцији заштите.....	48
9.1. Форензика мобилних уређаја	48
9.2. Прикупљање доказа са мобилних уређаја.....	48
9.3. Алати за прикупљање доказа.....	53
10. Пример прикупљања података са мобилног телефона.....	54
11. Сценарио – форензика мобилног телефона осумњиченог	63
11.1. Форензичка анализа мобилног телефона	65
12. Закључак.....	71
13. Литература.....	73

Садржај слика, табела и графика

Слика 1. Рудолф Арчибалд Рајс	14
Слика 2. 10 најпознатијих антифорензичких алата	20
Слика 3. Forensic Toolkit – FTK.....	29
Слика 4. Почетни прозор програма	30
Слика 5. Филтери за претрагу	31
Слика 6. Подешавања "случаја"	31
Слика 7.Блок шема мобилног телефона	38
Слика 8. <i>Nokia 101</i> - први <i>GSM</i> телефон	38
Слика 9. Унутрашњост УСБ стика	40
Слика 10. <i>Smart Media</i> меморијска картица	41
Слика 11. <i>xD-Picture</i> картице	41
Слика 12. <i>Secure Digital</i> картице	41

Слика 13. Псион 3	42
Слика 14. Nokia 9000 Communicator	43
Слика 15. Различити iPod уређаји.....	43
Слика 16. <i>USB Lock AP</i>	47
Слика 17. Производи који се користе - 1) <i>Cellebrite UFED</i> , 2) <i>Micro Systemation XRY</i>	49
Слика 18. <i>Micro Systemation XRY</i>	59
Слика 19. Тип аквизиције података	59
Слика 20. Логичка аквизиција	60
Слика 21. Процес прикупљања података.....	60
Слика 22. <i>General Information</i>	61
Слика 23. Белешке	62
Слика 24. СМС поруке	62
Слика 25. LG Optimus L9	64
Слика 26. Почетни екран програма	65
Слика 27. Врста података	65
Слика 28. Прикупљање података	66
Слика 29. Завршетак процеса прикупљања података.....	67
Слика 30. Дефинисање истраге	67
Слика 31. Прелазак на анализу	68
Слика 32. Креирање извештаја.....	68
Слика 33. СМС порука	69
Табела 1. Разлика између програма	29
Табела 2. Предности и мане алата	33

1. Методологија истраживачког пројекта

1.1. Уводне напомене и образложење рада

Са појавом персоналних рачунара дошло је до појаве првих дигиталних злочина. Врло брзо су људи проналазили рупе у оперативним системима и разним програмима и на разне начине, најчешће путем интернета, чинили велики број илегалних радњи. У данашње време те илегалне *on-line* радње су формирале посебну област криминала - „cyber“ криминал. Како се овакав криминал не може сузбити без криваца, а до њих се не може доћи само путем ДНК анализа, дошло је време да се оформи нови вид прикупљања доказа са виртуелних места злочина. Та област која се бави прикупљањем дигиталних доказа је управо дигитална форензика, област којом се бави овај рад. Описана је историја саме форензике, као и дигиталне форензике која је тема рада, затим и форензика мобилних телефона. Наведени су први случајеви који су решавани на овај начин, како су осумњичени били кажњени итд. Једно поглавље је посвећено и врсти криминала којом се бави дигитална форензика – компјутерски криминал. Описан је и један од најраспрострањенијих алата из ове области, са својим предностима и манама. Такође, појашњени су основни појмови дигиталне форензике и дигиталне форензике мобилних телефона као и један од често коришћених алата у овој области.

Овај мастер рад има циљ да обради основне појмови и чињенице везане за дигиталну форензику. Рад се састоји из три дела. Први део обухвата поглавља од другог закључно са шестим.

Друго поглавље је посвећено настанку дигиталне форензике и њеном развоју. Када се јавила потреба за дигиталном форензиком и зашто? На који начин се у почетку долазило до дигиталних доказа и шта су били први доказани злочини? Како се формирао закон за овакве преступнике?

Треће поглавље се бави основним појмовима из света дигиталне форензике. Биће објашњено шта се сматра дигиталним злочином, шта је то дигитални доказ, како се они прикупљају помоћу којих алата итд.

У четвртом поглављу је објашњен сам појам „cyber“ криминала, који су његови појавни облици и који од њих су најраспрострањенији.

У петом поглављу је описан принцип рада дигиталне форензике и како се прикупљају докази. Такође, наведени су и програми и алати који се користе. Описан је један од најкоришћенијих програма у овој области.

Шесто поглавље је окренуто регионалном стању дигиталне форензике и копјутерског криминала. Који то закони регулишу дигитални криминал и на који начин, какав је ниво свести о овом типу криминала и које и за шта први у Србији осуђен за неки дигитални злочин. Колико је стварно дигитална форензика развијена на нашим просторима.

Овде почиње други део рада који се бави ужом облашћу од дигиталне форензике – дигитална форензика мобилних уређаја. Обухвата поглавља почев од седмог па све до десетог, закључно са њим. Мобилни уређаји сваког дана постају све распрострањенији и приступачнији. Просечан човек данас поседује више од два мобилна уређаја и користи их сваки дан. То су мобилни телефони, таблет рачунари, *PDA* уређаји, *GPS* алати, *MP3* плејери, *USB* и остале меморије које се заснивају на флеш меморијама, итд.

Седмо поглавље нас упознаје са мобилним уређајима, шта су, како су настали и докле су стигли са развојом, и шта значе у једној истрази.

Осмо поглавље се бави заштитом мобилних уређаја, на који начин се делимично можемо обезбедити против разних врста злочина који се могу извести над неким мобилним уређајем.

Девето поглавље се бави форензиком мобилних уређаја тј. у овом поглављу ће бити објашњено на који начин се могу подаци прикупити са неког мобилног уређаја а десето поглавље нам даје једноставан пример како се један од најраспрострањенијих форензичких алата користи у ове сврхе.

На крају, трећи део рада преставља пример из праксе – реални сценарио форензичке истраге проневере новца у компанији *XYZ*. Биће показано над реалним подацима како их прикупити и анализирати.

Након овога, дванаесто поглавље је резервисано за закључак овог рада, а тринаесто за литературу, корисне линкове и референце.

1.2. Предмет истраживања

Предмет истраживања овог рада су основни појмови, чињенице и начела из света дигиталне форензике и суштина ове науке. Почетак рада је оријентисан ка историји форензике, ка настанку рачунара и развоју дигиталног криминала, па након њега и дигиталне форензике, затим се даље наводе основни појмови дигиталне форензике, објашњава се појам компјутерског криминала, његови појавни облици али и начини на који је он регулисан у свету и Србији и даје се пример коришћења једног форензичког алата. Такође, тема рада је и форензичка аквизиција података на мобилним уређајима. Форензичка аквизиција на малим уређајима се може вршити на различите начине, у зависности од тога који је уређај у питању. Чак се већина уређаја обрађује на сличне начине и са сличним алатима јер се заснивају на истим платформама (оперативни системи). Такође се неки уређаји обрађују као класични персонални рачунари због природе својих система.

Дат је пример логичке аквизиције података са мобилног телефона уз помоћ једног од популарнијих програма за форензичку истрагу.

1.3. Циљеви и задаци истраживања

Циљ рада је да прикаже основне појмове дигиталне форензике и да послужи као увод у науку, а затим и да разјасни и њену грану истраживања кроз реалан пример. Да би се неки дигитални злочин решио морају се идентификовати докази на прави начин и исто тако се они морају прикупити на прихватљив начин и врло пажљиво јер су то докази који су обично у несталном облику и могу се врло лако изгубити или нестати. Зато се мора знати тачан поступак њиховог безбедног прикупљања ради одржавања интегритета података. Задатак овог рада је да прикаже које су то стандардне процедуре за прикупљање доказа и на који начин се ти прикупљени докази анализирају и уопште како се користе. Који су то алати намењени томе и ко их обично користи по којој цени.

1.4. Истраживачке хипотезе

Општа хипотеза 1: починилац дигиталног злочина може бити било ко, па чак и запослени у компанијама жртвама. Постоји више начина на које неко може да почини неки дигитални злочин. Такође, постоји више начина на које подаци могу да се заштите од напада, или када већ до напада дође, да се докази о нападу прикупе и сачувају.

Радна хипотеза 1: полазећи од хипотезе да се злочин већ догодио, форензичар излази на терен да прикупи податке о свему што се десило. Након прикупљања доказа прави се временска линија тока догађаја. Касније се ти докази пореде са већ постојећим анализираним подацима или са сличним доказима прикупљеним на различитим уређајима.

На основу резултата форензичар реконструише след догађаја који се десио на том месту злочина.

Општа хипотеза 2: Извршиоци злочина над мобилним уређајима може бити неко ко му приступа физички и локално на лицу места или му може приступити у тренутку приступа интернету. Са обе стране је неопходно заштитити уређај, од локалног приступа неком врстом генеричке лозинке за приступ систему, а од мрежног приступа уз помоћ неких заштитних метода попут приступа сигурној мрежи, сигурним провереним продавницама апликација, итд. Такође су ту и опције да се поверљиви и јединствени подаци не чувају на мобилном уређају.

Радна хипотеза 2: Ако узмемо да се злочин већ десио, потребно је учинити све да би се преостали подаци и трагови на уређају на прави начин истражили, сачували и обрадили. Ту на сцену ступа форензичар са неким од многобројних алата за форензичку истрагу мобилних уређаја и тада долази до закључка да је дати уређај био мета, мотив, оруђе или доказ злочина.

1.5. Методе истраживања и ток истраживачког процеса

У токе истраживања се пролази кроз четири фазе: постављање проблема, формулисање хипотезе, њена провера и потврђивање тј. верификација хипотезе. Истраживачки процес чине два дела – само истраживање и презентација добијених резултата.

У овом раду су подаци прикупљени деск методом истраживања – коришћени су већ прикупљени подаци али у другачијем обиму и облику. Такође се од тих података, дедукцијом и индукцијом, дошло до резултата и закључака наведених у раду.

2. Порекло и корени дигиталне форензике

*"Компјутерска форензика је очување, идентификација, екстракција, тумачење и документација рачунарског доказа."*¹

Компјутерска форензика је дисциплина која има за циљ да прикупи, сачува и презентује податке који су добијени са медија за чување података (хард диск, *CD ROM*, *DVD ROM*, дискета, усб стик итд.). Комбинујући елементе права и компјутерске науке сакупља и анализира податке који се даље користе као докази на суду. Користи сличне технике које се подразумевају приликом спасавања података са додатком смерница за примену у правном поступку.² У наставку рада ће бити приказани неки од алата који се користе у прикупљању доказа.

Дигитална форензика се као наука развила релативно скоро, спада у млађе научне области. Сама форензика вуче корене још из Римског доба када су кривичне пријаве подразумевале јавно изношење случаја у Форуму, где би лице оптужено за кривично дело и подносилац пријаве јавно расправљали о овоме а особа са бољом аргументацијом и презентацијом би превладала. Отуда и порекло самог назива форензика од латинске речи *forēnsis* што значи "пред форумом". Први писани документ о употреби медицине и ентомологије у решавању кривичних предмета, приписује се књизи Хи Јуан Лу (宋慈, 1186.–1249.) која је објављена 1248. године. Након тога, много година касније је шведски хемичар Карл Вилхелм Шил (*Carl Wilhelm Scheele*, 1742.-1786.) 1773. године осмислио начин откривања арсена у лешевима али само у великој количини. После њега је та истраживања наставио немачки хемичар Валентин Рос (*Valentin Ross*) 1806. Када је успео да открије отров у зидовима желуца жртве. Прва забележена употреба отисака прстију од стране полиције као доказни материјал је била када је Жуан Вуцетич (*Juan Vucetich*, 1858.-1925.) у Аргентини решио случај убиства коришћењем крвавог отиска прста који се

¹ [1] The Best Damn Cybercrime and Digital Forensics book Period, Anthony Reyes, Jack Wiles, 2007.

² [13] <http://www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-osnove.htm>

налазио на узорку коже скинутог одсецањем дела врата на коме су се отисци налазили.



Прва школа форензике је отворена у Европи, у Лозани (Швајцарска) и то од стране Рудолфа Арчибалда Рајса (*Rodolphe Archibald Reiss*, 1875.-1929.) 1909. године.

Што се тиче дигиталне форензике историја је мало другачија. Сами рачунари су се појавили тек средином XX века. И тада када су се појавили рачунари још увек није било интернета па ни самог дигиталног криминала па за форензиком тог типа није било потребе.

Прво почетком седамдесетих година XX века, са појавом интернета, и касније почетком осамдесетих година, када персонални рачунари постају приступачнији, долази до њихове све веће злоупотребе, тј. повећања употребе компјутера приликом извршења криминалних радњи. Због тога је Федерални истражни биро (*Federal Bureau of Investigation - FBI*) 1984. године оформио нову јединицу *Computer Analysis and Response Team (CART)* која је имала за циљ да се избори са све већим бројем случајева који су укључивали дигиталне доказе. У компјутерске злочине спадају хаковање, дечија порнографија, компјутерске преваре, саботаже, крађа идентитета итд.

ASCLD-LAB друштво (*American Society of Crime Laboratory Directors/ Laboratory Accreditation Board*) је 2003. године прихватило појам дигиталне форензике и значај дигиталног доказа у решавању злочина, док је Канада прва земља која је 1983. године донела закон који делимично регулише дигитални злочин, након њих следи Америка 1986., затим Аустралија 1989. године а потом и Енглеска 1990. године. Од тада се повећало интересовање за едукацијом и жеља за унапређењем ове новонастале науке. Данас, у Сједињеним Америчким Државама постоји више десетина колеџа који су специјализовани за ову област. САД је тренутно лидер у овој области.³ Иако би се могло очекивати да

³ [28] http://en.wikipedia.org/wiki/Digital_forensics

је Србија технолошки заостала земља, то није случај. Налази се на трећем месту у свету по преварама путем интернета.

Иако је дигитална форензика призната тек пре неколико година, први забележени напад на неку дигиталну инфраструктуру се десио 1988. године од стране Роберта Мориса. Он је пронашао грешку у једном рачунарском систему и уз помоћ вируса "срушио" 6000 рачунара на интернету. Због тога је морао да плати одштету од 10.000 долара, добио је казну од три године затвора и 400 сати добровољно корисног друштвеног рада.⁴

Форензика и њена грана, дигитална форензика, су постале популарне почетком деведесетих година прошлог века са појавом првих телевизијских серија на ову тему: *Crime Scene Investigation, Criminal Minds, Dexter, Law & Order, Forensic Files* итд.

Раст компјутерског криминала током 1980-их и 1990-их година је приморао тзв. агенције за спровођење закона да почну да формирају специјализоване групе да рукују техничким аспектима истраге. Једна од првих забележених примена дигиталне форензике је када је Клиф Стол (Cliff Stoll) трагао за хакером Маркусом Хесом (Markus Hess) 1986. године. Стол није био специјализован за овакав вид истраге али је користио технике компјутерске и мрежне форензике у својој истрази. Током 1990-их година дошло је велике потражње за овим новим видовима истраге. Дошло је до формирања многих регионалних, па чак и локалних јединица које ће се бавити дигиталном форензиком.

Тек 1992. године термин "дигитална форензика" почиње да се користи у стручној литератури, од стране Колиера (Collier) и Спаула (Spaul) који су први у свом раду покушали да објасне овај појам и оправдају га свету. Брз развој дигиталне форензике је узроковао недостатак стандардизације и обуке у овој области. Неки од првих писаних радова везаних за ову област су издати тек након 2000. године. Радна група за дигиталне доказе (The Scientific Working Group on Digital Evidence (SWGDE)) је 2002. године издала рад на тему "Најбоље примене компјутерске форензике", након тога издат је ИСО стандард 2005.

⁴ [2] Семинар о *Cyber*тероризму – „Кризе и кризно управљање“, Хрватска, 27.03.2012.

године (ИСО 17025, Општи захтеви за компетентност лабораторије за тестирања и калибрације). Конвенција о високотехнолошком криминалу је ступила на снагу 2004. године, са циљем усклађивања националних закона који регулишу компјутерски криминал, истражне технике и међународну сарадњу. Споразум су потписале 43 земље (укључујући САД, Канаду, Јапан, Јужну Африку, Велику Британију итд.) а ратификован је од стране 16 земаља.

Након ових неколико година фокус се потпуно пребацио на интернет криминал и интернет тероризам. Дигитална форензика се и даље суочава са много нерешених питања. Симсон Гарфинкел (Simson Garfinkel, 1965-) је 2010. године идентификовао проблеме са којима ће се суочавати дигитална форензика у будућности који укључују повећање капацитета дигиталних медија, широку доступност шифровања обичним корисницима, велики број варијанти оперативних система и формата датотека као и све већи број појединаца који поседују више од једног уређаја, као и правна ограничења над истражитељима.

3. Основни појмови дигиталне форензике

Основни појмови дигиталне форензике су паралелни са основним појмовима њеног тзв. "родитеља" - форензике, само са префиксом дигитални.

Дигитална форензика⁵ - основна дефиниција је да је дигитална форензика вид систематске контроле компјутерског система, и садржаја истог, ради прикупљања доказа о извршеном кривичном делу или некој другој злоупотреби, у чијем је извођењу учествовао рачунарски систем.

Такође представља примену рачунарске науке и математике за поуздано и непристрасно прикупљање, анализу, интерпретацију и презентацију дигиталних доказа за потребе реконструкције догађаја који је окарактерисан као криминално дело или као помоћ код предвиђања и превенције неауторизованих догађаја и акција.

⁵ [29] http://sr.wikipedia.org/sr/digitalna_forenzika_i_alati

Дигитална форензика се може поделити на рачунарску, форензику мобилних уређаја, мрежну и форензику база података. У зависности од области дигиталне форензике користе се различити алати који се осим по области могу поделити и по начину имплементације, типу кода, платформи на којој раде и према фази процеса коју обављају у истрази. О врстама и самим алатима ће бити речи у наредним поглављима рада.

Дигитална форензика има широку примену и није ограничена само на полицијско-судске и војно-обавештајне активности. Банкарски сектор, осигуравајућа друштва и компаније разних профила имају потребу и морају бити изузетно опрезни са подацима којима располажу јер је многим компанијама нанесена немерљива штета због индустријске шпијунаже и генералне злоупотребе ИТ система. Напад увек има већи изглед да успе уколико се изведе изнутра и зато озбиљне компаније не штеде на заштити од "инсајдера", односно запослених унутар фирме који су спремни да раде за конкуренцију или да нанесу штету матичној фирми из неких других разлога.

Дигитални доказ⁶ - представља информацију од значаја за истрагу, а која је складиштена у дигиталној форми. Оригинални доказ треба да буде сачуван у оригиналном или што приближнијем стању. Ако је потребно даље испитивање оно се врши над копијом која мора бити прецизно направљена и складиштена на „форензички стерилном“ медијуму (медијум на којем претходно није било података). Сви докази морају бити прописно означени и документовани. Ако су подаци обрисани или оштећени, употребом одређеног софтвера могуће их је повратити. Тај процес може трајати дуго ако је изгубљен или оштећен велики број података.

У дигиталне доказе спадају дигитални видео и аудио сигнали, записи са дигиталне факс машине, дигиталне камере или фото апарата, разних мобилних уређаја итд. Неки дигитални материјал постаје доказ оног тренутка када га суд призна и када се он прикупи на легалан начин. Суд одлучује да ли је тај материјал релевантан за истрагу и да ли је материјал аутентичан. Осим суда

⁶ [30] http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf

доказ "користе" још и тужилаштво, осигуравајући заводи, званични истражни органи (МУП, БИА, итд.), власници нападнутог ИТ система итд.

Дигитални, као и "обичан" доказ може показати различите ствари: када се догађај десио, на ком месту, од стране кога, ко је жртва, шта се десило, који је мотив и сама намера извршења злочина итд.

Како се све више рачунари развијају тако стварају проблеме у дигиталним доказима. У прво време дигитални докази су вредели много више него што можда сада неке врсте вреде. Сада, када је на рачунару могуће изменити све, пре свега дигиталне фотографије и видео снимци губе свој значај и морају проћи кроз многе провере. Када се доказ прикупи, све акције које се обављају над и са тим доказом морају бити документоване ради праћена било каквих евентуалних промена.

Дигитални подаци који су кандидати за дигиталне доказе се могу категорисати на следећи начин:

- **Прелазни подаци** - резидентни програми, њихов животни век се завршава гашењем рачунара;
- **Осетљиви подаци** - налазе се на хард диску рачунара и подложни су накнадним променама;
- **Привремено приступачни подаци** - подаци на локалној машини којима се приступа искључиво у унапред одређено време.

Дигитални подаци се могу уништити или намерно брисањем или гашењем рачунара, када може доћи до брисања података. С обзиром да на интернету постоји доста и бесплатних и комерцијалних програма који служе за враћање изгубљених података на неки жељени медијум. Уколико дође до физичког рециклирања медијума на коме се налазе подаци, њихов повраћај није могућ.

Дигитални злочин⁷ — се односи на било који злочин који укључује рачунар и мрежу. Рачунар је можда коришћен у извршењу кривичног дела, или може да буде мета. Године 2011. дигитални криминал је дефинисан као: дела која су

⁷ [31] http://www.dataprotection2003.info/speakers/Marijan_Risteski/presentation.pdf

почињена против појединаца или група појединаца са криминалним мотивом да намерно повреди углед жртве или да изазове физичке или психичке повреди жртве директно или индиректно, коришћењем модерне телекомуникационе мреже - интернет (чет собе, е-маил поруке) и мобилни телефони (СМС/ММС). Дигитални злочин може бити упад⁸, кршење ауторских права, дечија порнографија, и разне обмане. Јављају се и проблеми приватности када се поверљиве информације изгубе или буду пресретнуте, шпијунажа, финансијске крађе и друге пограничне злочине. Генерално, сви злочини се могу поделити у две категорије: злочини којима је мета директно рачунар (вируси, *DOS*⁹ напади, *malware* итд.) и злочини који користе рачунарске мреже или уређаје као посреднике да остваре више циљеве (сајбер прогањање, превара или крађа идентитета итд.).

Неки од најраспрострањенијих интернет злочина:

Spam – нежељено и насумично слање рекламних е-маил порука у комерцијалне сврхе.

Превара – свако неискрено представљање чињеница са намером да изазове различите реакције код жртве којима ће она остати без својих личних података или можда и новца.

Непристојан или увредљив садржај - садржај веб сајтова и других начина електронске комуникације може да буде неукусан, непристојан или увредљивиз разних разлога. У неким случајевима та комуникација може бити незаконита. У којој мери су те комуникације незаконите варира између земаља. Једна област интернет порнографије која је била мета најјачих напора за сузбијање је свакако дечија порнографија.

Узнемиравање - док садржај може бити увредљив, малтретирање усмерава увредљиве коментаре на конкретне појединце са фокусом на његове особине, нпр. на пол, расу, веру, националност, сексуалну оријентацију. То се често дешава у собама за четовање или слањем е-маил-а мржње кључним странама

⁸Добијање неауторизованог приступа рачунару у циљу брисања података у том систему.

⁹***Denial-of-service*** – напад који чини персонални рачунар или мрежу недоступним за свог крајњег корисника.

(сајбер ухођења, злочин из мржње итд.). Сваки коментар који се може идентификовати као погрдан или увредљив, сматра се узнемиравањем.

Такође се појављују случајеви продаје дроге, многих црних тржишта попут продаје органа, лекова итд, као и сајбер тероризам.

Дигитално место злочина¹⁰ - рачунар који је под истрагом и на коме се десио злочин се може сматрати дигиталним местом злочина. Физички докази могу постојати око сервера који је нападнут од стране запослених и може постојати доказ о коришћењу ококућног рачунара који садржи недозвољене податке. Циљ већине дигиталних истрага је да идентификује особу која је одговорна за тај злочин и стога дигитална истрага треба да буде уско повезана са физичком истрагом.

Анти-форензика – је скуп алата и техника којима се хакери бране од форензичке истраге и помоћу њих је отежавају или онемогућавају. Кад је реч о програмима који се користе на *Windows* платформи, њихово подешавање у *Control Panel* – у или самом том програму може знатно ометати истрагу, може доћи до брисања привремених података, историје прегледа на интернету, брисање поште из сандучета итд. Такође, то се све може учинити посебним програмима који се могу наћи на интернету а који служе за прикривање трагова коришћења рачунара а то отежава истрагу.

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	
Excellent Very Good Good Fair Poor	Webroot Window Washer 	CyberScrub Privacy Suite 	Evidence Eliminator 	Privacy Guardian 	ParetoLogic Privacy Controls 	WinSweeper 	GhostSurf 	Anti Tracks 	Privacy Protector 	History Clean 	
Reviewer Comments	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	
Lowest Price	BUY \$29.95	BUY \$59.95	BUY \$99.95	BUY \$29.95	BUY \$39.95	BUY \$39.95	BUY \$39.95	BUY \$34.95	BUY \$29.95	BUY \$19.90	
Overall Rating											

Слика 2. 10 најпознатијих антифорензичких алата

¹⁰ [32] <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>

4. *Cyber* криминал¹¹

Компјутерски криминал (*cyber* криминал) је појава новијег времена, посебан вид криминалитета који је постао глобални проблем. Под компјутерским криминалом обично се подразумева криминалитет који ангажује компјутер као средство или као циљ извршења кривичних дела. У основи је реч опостојећим облицима криминала који чине људи, а не рачунари. То није само још један облик обичног криминала, већ је то општи вид свих облика криминала.

Компјутери и компјутерска технологија се могу злоупотребљавати на разне начине, а сам криминалитет који се реализује помоћу компјутера може имати облик било ког од традиционалних видова криминалитета, као што су крађе, утаје, проневере, док се подаци који се неовлашћено прибављају злоупотребом информационих система могу на разне начине користити за стицање противправне користи. Термин сајбер простор први је употребио Вилијам Гибсон (*William Gibson*, 17.03.1948.-) у научно-фантастичној новели Неуромансер (*Neuromancer*) 1984. године.

Проблеми неовлашћеног приступа приватним информацијама скренули су пажњу на могућност коришћења рачунара у сврхе привредног криминала. У периоду од јуна до августа 1994. у осамнаест упада Владимир Левин је извукао преко 10 милиона долара из система Ситибанк (*Citybank*). Наредне године је ухапшен у Лондону, 1997. изручен америчким властима, а у августу исте године је осуђен на 36 месеци затвора и казну од 250.000 долара. Кевин Митник у САД је ухапшен и осуђен 1995. године за фалсификовање 20.000 бројева кредитних картица.

Са повећаном употребом персоналних рачунара повећала се и брига за заштитом од неовлашћеног приступа рачунарским подацима. Све већа умреженост је увеличала ту бригу и довела до нових проблема, попут напада на удаљене рачунаре и мреже, и у кривични систем додала дела као што су повреде ауторских права, дистрибуција дечје порнографије итд.

¹¹ [31] http://www.dataprotection2003.info/speakers/Marijan_Risteski/presentation.pdf

Постоје две категорије овог криминала:

- Компјутерски криминал у ужем смислу - свако незаконито понашање усмерено на електронске операције сигурности рачунарских система и података који се у њима обрађују;
- Компјутерски криминал у ширем смислу - као свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминал какво је незаконито поседовање, нуђење и дистрибуирање информација преко компјутерских система и мрежа.

Конкретни облици овог криминала:

- Неауторизовани приступ рачунарском систему или мрежи кршењем мера сигурности (хаковање (*hacking*));
- Оштећење компјутерских података или програма;
- Компјутерске саботаже;
- Неовлашћено пресретање комуникација од и у компјутерским системима и мрежама;
- Компјутерска шпијунажа.

Сваки од ових облика може се укрштати са сваким јер готово да не постоји "чисти" облик. Тако хаковање, поред неовлашћеног уласка у компјутерске системе и мреже, често обухвата и уништење података или компјутерску шпијунажу (као што је то случај са упадима на веб сајтове и уништење или "преправљање" података на њима или трговина података са приступ систему). Измена компјутерских података и програма укључује и покретање компјутерских црва и вируса што је најчешће праћено заустављањем рада компјутерског система, уништењем података итд. У мрежама црви и вируси се у већини случајева прослеђују електронском поштом, а некада их и хакери убаце непримећено у систем приликом неовлашћеног приступа.

Од дела рачунарског криминала у ширем смислу најчешће се појављују:

- Фалсификати
- Компјутерске крађе

- Техничке манипулације уређајима или електронским компонентама уређаја
- Злоупотребе система плаћања као што су манипулације и крађе електронских кредитних картица или коришћење лажних шифри у незаконитим финансијским активностима.

У ова дела се убрајају разни незаконити и штетни садржаји, кршење ауторских права, продаја забрањене робе (оружја, крадене робе, лекова) или пружање недозвољених услуга (коцкање, проституција). Највише пажње у овој групи дела привлачи дечија порнографија и дистрибуција разних материјала Интернетом.

Европска конвенција о високотехнолошком¹² криминалу предвиђа 4 групе дела:

1. Дела против поверљивости, интегритета и доступности компјутерских података и система – њихчине незаконити приступ, пресретање, уплитање у податке или системе, коришћење уређаја (производња, продаја, увоз, дистрибуција), програма, података за логовање на систем;
2. Дела везана за компјутере – код којих су фалсификовање и крађе најтипичнији облици напада;
3. Дела везана за садржаје – дечија порнографија је најчешћи садржај који се појављује у овој групи обухватајући поседовање, дистрибуцију, трансмисију, чување или чињење доступним и расположивим ових материјала, њихова производња ради дистрибуције и обрада у компјутерском систему или на носиоцу података;
4. Дела везана за кршење ауторских и сродних права обухватају репродуковање и дистрибуцију неауторизованих примерака дела компјутерским системима.

Зависно од типа почињених дела компјутерски криминал може бити:

- Политички:

¹² [3] Конвенција о високотехнолошком криминалу, Будимпешта, 23.11.2001.

- o шпијунажа и саботажа у свету рачунара
- o хаковање (основе безбедности на интернету, основе заштите од компјутерских вируса)
- o тероризам (асиметрични виртуелни рат, интернет као оружје терориста)
- o ратовање (ампликације евентуалног оружаног сукоба)
- Економски:
 - o преваре („Нигеријска подвала“¹³ или прање новца)
 - o крађа интернет времена, крађа интернет услуга
 - o производња и дистрибуција недозвољених садржаја као што су дечија порнографија, педофилија, верске секте, ширење расистичких, нацистичких и сличних идеја и ставова (Џихад преко интернета)
 - o злоупотреба жена и деце
 - o манипулација забрањеним супстанцама и робама: дрогом, људским органима, оружјем
 - o повреде приватности: надгледање е-поште, „спам“, „пецање“¹⁴, снимање разговора у чет собама,
 - o праћење е-конференција, прикачињање и анализа шпијунских софтвера.

¹³ Писма наводног сина бившег председника Либерije у коме тражи помоћ око пребацивања велике своте новца са једног рачуна на рачун потенцијалне жртве

¹⁴ Подразумева вид преваре на интернету која се обично одвија тако што преварант шаље другима е-пошту где се представљао као власник фирме (наравно, непостојеће) не би ли их преварио и дошао до њихових података који ће му послужити за крађу идентитета.

5. Принцип дигиталне форензичке истраге¹⁵

Дигитална форензичка истрага се заснива на принципима дигиталне форензичке науке и подразумева употребу уобичајених форензичких техника, рачунара и разних програма за форензичку истрагу.

5.1. Прикупљање дигиталног доказа

Када се деси дигитални злочин, процедура прикупљања доказа се врши на сличан начин на који се прикупљају и класични докази на неком месту злочина. Такође се ради увиђај, дигитални форензичари излазе на место злочина и пре свега фотографишу затекнуто стање и пишу извештаје са свим релевантним информацијама које се тичу тог злочина. Те релевантне информације се састоје из локације на којој се злочин десио - тип рачунара, његову додатну опрему и конфигурацију, и из списка свих бежичних и жичаних веза између медијума на којима се десио злочин. Оно што је веома битно јесте да се медијум оставља у стању у коме је затекнут, уколико је реч у укљученом рачунару он се не сме никако гасити јер може доћи до оштећења дигиталних доказа тј. до њиховог трајног губљења уколико се налазе у радној меморији. Када се након снимања затеченог стања пређе на процес одношења медијума са места злочина потребно је фотографисати монитор у затеченом стању па га уклонити. Такође потребно је направити копију свих медијума, пре свега хард диска, пажљиво угасити рачунар и пре одношења фотографисати све периферне уређаје који су повезани на рачунар, развезати све те уређаје и обележити начине на који су били спојени на рачунар и све делове рачунара ставити у за то предвиђене кутије и кесице и пренети у лабораторију на даља испитивања. Битан фактор код прикупљања доказа је и жртва злочина тј. власник рачунара. Његово присуство је неопходно због познавања тог система и свих потребних података за приступање систему - корисничка имена и шифре, налоге за приступ, коришћене методе заштите података и многе друге информације о разним подешавањима рачунара. Дешава се да корисник не жели да даје такве информације и тако је потребно извадити судске налоге за пун приступ подацима.

¹⁵ [32] <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>

Када се докази прикупе на месту злочина и транспортују у лабораторију, приступа се претраживању прикупљених података па након тога њихова детаљна анализа.

Код прикупљања доказа морају се поштовати одређени стандарди везани за руковање дигиталним доказима:

- Оригинални доказ треба бити сачуван у оригиналном стању или стању што приближнијем оном у моменту проналажења,
- Ако је могуће потребно је направити прецизну копију (слику) оригинала да би се на копији вршило испитивање и, на тај начин, сачувао и заштитио интегритет оригинала,
- Копије података направљених у сврху испитивања треба да буду креиране на форензички стерилном медијуму,
- Сви докази и сваки корак форензичког испитивања морају бити прописно означени и документовани.

5.2. Алати за прикупљање дигиталних доказа¹⁶

Алати који се користе за прикупљање дигиталних доказа су алати за саму детекцију података, за њихову анализу, проверу аутентичности итд. Неки од њих се могу бесплатно преузети са интернета, док су остали комерцијалног типа. Постоји више категорија алата за дигиталну форензику. Могу се поделити према начину имплементације, према области употребе, према типу кода, према платформи на којој ради као и према фази у којој се користи у оквиру форензичке истраге.

- Према начину имплементације
 - хардверске алате
 - програмске (софтверске) алате
- Према области употребе
 - алате за форензику рачунарске мреже
 - алате за форензику рачунарског система

¹⁶ [33] <http://www.infoteh.rs.ba/rad/2012/RSS-4/RSS-4-9.pdf>

- o алате за анализу других дигиталних уређаја (нпр. ПДА, мобилних телефона, итд.)
 - o алате за форензику софтвера (малициозних кодова)
- Према типу кода
 - o програмске алате отвореног кода
 - o лиценциране програмске алате
- Према платформи на којој раде
 - o алате који раде на виндоус платформи
 - o алате који раде на линуксу и другим платформама
- Према фази процеса који обављају у форензичкој истрази
 - o алате за прављење стерилних медијума
 - o алате за прављење физичке копије чврстог диска
 - o алате за опоравак података
 - o алате за дешифровање података (разбијање шифара)
 - o алате за анализу дигиталног материјала
 - o алате за документовање

Неки од најраспрострањенијих алата у овој области који се користе на рачунарима су *EnCase, Safe Back, Access Data, Driver Spy, Data Decoder, Scalpel* – *Open Source* alat. Alati koji se koriste na mobilnim telefonima, PDA uređajima i za SIM kartice: *Cellibrite UFED, Bit PIM*.

Неки од алата који се користе за преглед свих података на рачунарском систему су: *SafeBack, DIBS, Maresware, NTI* итд. Алати за праћење мрежног саобраћаја: *Carnivore, NetIntercept, NetWitness* итд. Алати за приступ подацима који се налазе под заштитом (шифра) и подацима који су избрисани: *ZERT, TULP, Cards4Labs* итд.

EnCase – програмски алат намењен форензичкој истрази дигиталних доказа фирме *Guidance Software*. Користи се од стране многих водећих компанија и организација у области дигиталне форензике. Омогућава и олакшава судским вештацима и ИТ стручњацима истраживање случајева, аквизицију и анализу доказног материјала и што је свакако најважније за ИТ вештаке јесте да не омогућава измену података преузетих са корумпираног рачунара. Најновија

верзија овог алата је доступна само владиним и образовним институцијама. Кључ за откључавање овог софтвера је УСБ уређај.

DriveSpy – форензички алат за ДОС оперативни систем који је развила компанија *Digital Intelligence*. Иако нема развијен графички интерфејс алат је доста популаран међу форензичарима јер је програм величине само 11кб и лако је преносив на свим медијима. Иначе ради се о алату који проширује основе МС-ДОС функције, а садржи све потребно за копирање и испитивање садржаја диска. Додатне функције су и креирање МД5 хеша за копирани диск, партицију или изабране датотеке, сигурно брисање диска. Последња верзија садржи додатак који омогућава приступ и рад са УСБ флеш дисковима, док приступ осталим меморијским картицама зависи од произвођача, читача, типа и слично.

Helix – своју популарност дугује и томе што је до последње верзије (објављене у марту 2009. године) био потпуно бесплатан. Његова најновија верзија, која се за разлику од претходних, које су се заснивале на *Knoppix* дистрибуцији, заснива се на *Ubuntu Linux*. У најповољнијем облику кошта 239 долара годишње (искључиво за академске институције). *Helix* спада у групу софтвера намењених раду директно са *CD-ROM* медијума. Без обзира о којој се основној верзији линукса ради, *Helix* је модификован на начин да никад не користи свап (*swap*) партицију и да препознаје скоро све могуће фајл системе. Важна функционалност је и могућност покретања у облику самосталне апликације на *Windows* оперативним системима. *Helix* је подељен у програм који анализира подигнуте *Windows* системе и *Linux* оперативни систем који се самостално подиже.

VMware – популаран производ за виртуелизацију (*VMware Workstation 7.x* је актуелна верзија) који омогућава креирање псеудорачунара и псеудомрежа, који за све користе хардвер једног система. Може се подесити као гост оперативни систем, инсталирати потребни форензички алати, од њега направити слика система, радити на њему, а по потреби увек довести у преконфигурисано стање. Са њега је могуће извршити све врсте испитивања, укључујући инсталирање и праћење злонамерних програма, понављање

сигурносног инцидента. Када су у питању преносиве меморије, VMware нуди опцију да уређај уопште нема контакт са рачунаром домаћином.

Већ је споменута подела форензичких алата иако један алат може да припада не само једној, већ више група алата. Такође, неопходно је да алати неким делом кода буду отворени ради провера тачности резултата јер уколико докази нису правилно прикупљени, биће одбачени на суду. Главне разлике између програма отвореног кода (*open source*) и лиценцираних програма:

	<i>Open source</i> програми	Лиценцирани програми
Платформа	<i>Linux</i>	<i>Windows</i>
Корисничка подршка	Углавном не постоји	Пуна подршка
Покривеност области истраге	Углавном не покривају све области истраге	Пуна покривеност истраге

Табела 1. Разлика између програма

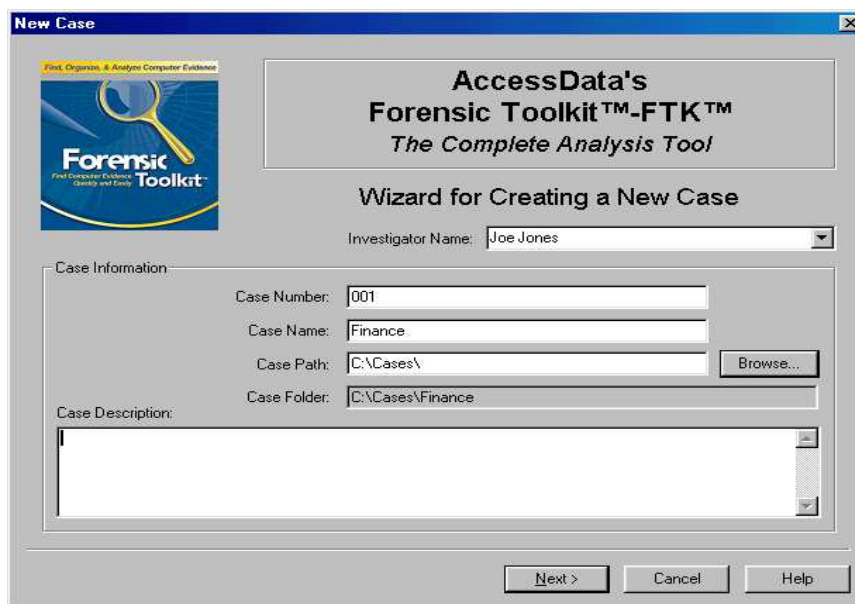
Већина програма који се користе у дигиталној форензичкој истрази су набројани у претходним поглављима. За пример је узет један од лиценцираних и популарних алата - *Forensic Toolkit-FTK*.

Forensic Toolkit (FTK)¹⁷ – један од најстаријих форензичких софтвера. Због графичког интерфејса и рада на Windows оперативним системима постао је веома популаран. Његов интегрални део, *FTK Imager* је можда и најпознатији софтверски алат за „бит по бит“ копирање, а који се може скинути и бесплатно са интернета. Сlike дискова направљене *FTK Imager* програмом признате су на суду као ваљани докази. Осим тога обједињује све остале постојеће формате за прављење форензичких копија.



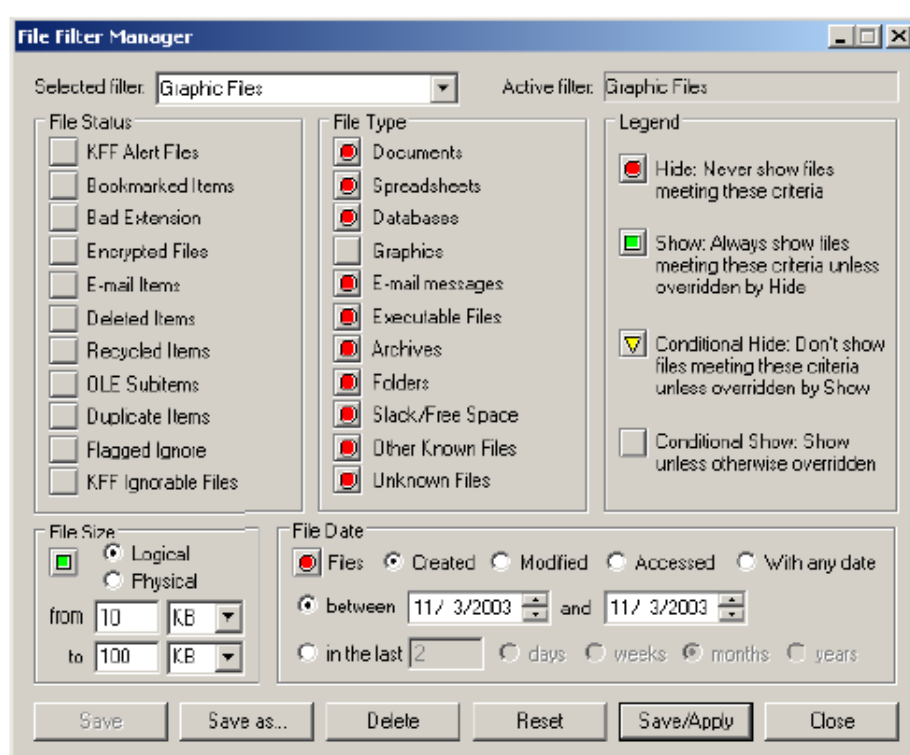
Слика 3. Forensic Toolkit – FTK

¹⁷ [34] <http://ad-pdf.s3.amazonaws.com/ImagerUsersGuide.pdf>



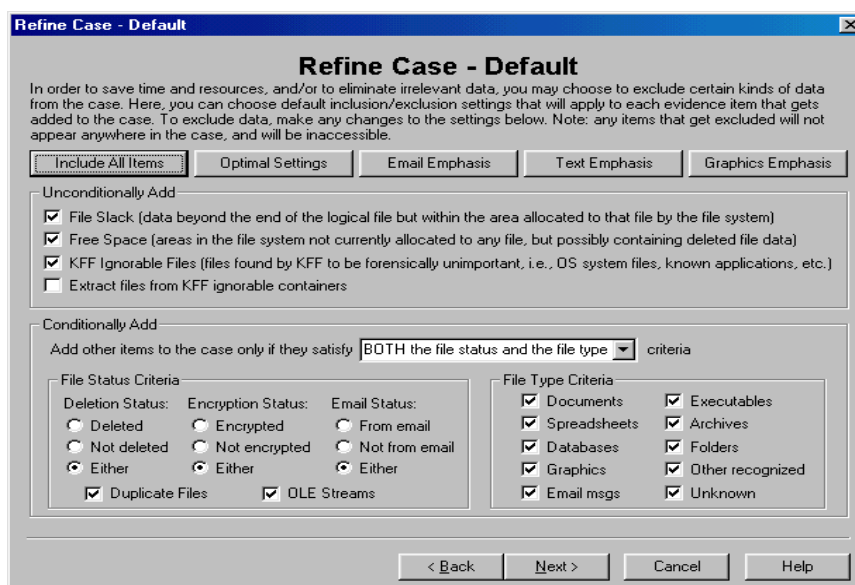
Слика 4. Почетни прозор програма

FTK се користи у истрагама као алтернатива алату *EnCase*. *FTK* омогућава корисницима да истраже и направе слику (*image*) тврдог диска (*HDD*) и то путем испитивања слика кроз галерију, испитивањем фајлова кроз хексадецимални поглед и претраживањем диска преко кључних речи. Садржи прилагодљиве филтере који омогућавају истражитељима да се крећу кроз хиљаде фајлова, е-пошту, као и лоцирање изгубљене и избрисане е-маилове (*Outlook, AOL, Outlook Express, Netscape, Earthlink, Yahoo, Hotmail, Eudora* и *MSN*). Омогућава приступ енкриптованим подацима и њихово декриптовање. Врши скенирање диска за текстуалне стрингове које касније користи као речник шифара за разбијање енкрипције података. Претраживање се врши на бази регуларних израза (*regular expressions*), садржи у себи већ дефинисане изразе за претрагу броја телефона, адреса итд.



Слика 5. Филтери за претрагу

Прављење слике диска се врши кроз његов додатак (*FTK Imager*). Слика диска се може направити или у једном фајлу или у сегментима који се после могу засебно користити и реконструисати. Алат је прихваћен на суду и направљен је да буде брз, аналитичан и скалабилан у односу на већину предузећа.



Слика 6. Подешавања "случаја"

Представља интегрисано решење за истрагу:

- Обрађује велики број типова података од форензичких слика до архива е-поште, анализира регистар, декриптује фајлове, разбија шифре и прави извештај о току истраге,
- Поседује опцију да обнови лозинку са више од 100 апликација,
- Садржи *KFF (KnownFileFilter)* хеш библиотеку са више од 45 милиона хешева,
- Одликује га напредна и аутоматизована анализа без скриптовања.

Подржава више од 700 типова слика, архива и фајлова и заснован је на бази података па не може доћи до прекида.

Представља једино форензичко решење које може да идентификује енкриптовани PDF фајл. Без проблема енкриптује *Credant, SafeBoot, Utimaco, Safe Guard Enterprise and Easy, EFS, PGP, Guardian Edge, Pointsec* и *S/MIME*. Садржи библиотеку са више од 30.000 слика које служе за аутоматску идентификацију потенцијално порнографских слика.

Одликује се богатим системом извештавања у више формата: *HTML, PDF, XML, RTF* и други. Користи посебан тип извештаја за проналазак фајлова који не могу да се обраде или да се индексирају - *Processing Exception/Case Info*. Такође може да креира и *CSI* фајлове који се могу касније превести у *Excel*.

Предности	Мане
- могућност анализе података са различитих извора - има једноставан кориснички интерфејс - брзо претраживање - додавање обележивача - извештавање - креирање речника шифара - креирање индекса кључних речи	- нема праћења прогреса истраге - нема мулти таскинг - нема подршке за скриптовање - постоји лимит фајлова – 2 милиона - нема временску линију осим за сортирање колона - прилично скуп алат: основна лиценца кошта \$795

- приказ е-поште у HTML формату (укључујући IP адресе, POP3 сервере и додатке пошти (<i>attachments</i>))	
---	--

Табела 2. Предности и мане алата

Пример коришћења: уколико се током форензичке истраге дође до рачунара који се сматра „местом злочина“, у алат се могу учитати слике са рачунара ради индексирања. Након овог процеса, може се видети колико слика, видео снимака и докумената постоји на рачунару и да ли постоје енкриптовани фајлови или они који нису значајни за истрагу. Фајлови се излиставају са посебним ознакама – „*KFF Узбуна*“ (*KFF Alert*) за фајлове који су неопходни за истрагу и „*KFF Небитан фајл*“ (*KFF Ignorable file*) за фајлове који су небитни за истрагу.

Главна предност овог алата је могућност претраге, користи посебну врсту претраге да би изградио целокупне текстуалне индексе за претрагу док неки други алати користе тзв. тренутну претрагу која може да траје сатима у зависности од тога колика је величина слика или диска.

6. Стање и напредак дигиталне форензике у Србији у борби против ИТ криминала

6.1. Високотехнолошки криминал у Србији

Ова посебна врста криминала се појавила на просторима бивше СФРЈ почетком осамдесетих година прошлог века када се откривају и гоне прва кривична дела, а која су за свој циљ имала прибављање противправне имовинске користи и то тако што су извршиоци запослени као систем администратори у јавним институцијама изменама програмског кода утицали на израду коначних обрачуна стања на банковним рачунима или обрачуна личних доходака и тиме увећавали своје приходе.

Иако су случајеви били ретки јер су рачунарски системи били претежно доступни институцијама и предузећима, тј. лицима која су била запослена у

истим, док се у власништву грађана налазио врло ограничени број рачунара намењених личној употреби.

Почетком деведесетих година стање у информационим технологијама у Србији се незнатно мења повећањем броја личних рачунара и пуштањем у рад *YUPAC* мреже која је имала могућност приступа Интернету.

Информациони криминалитет доживљава свој процват практично од средине деведесетих година и то из неколико разлога од којих су најбитнији следећи:

- број рачунара у јавној и личној употреби се повећава захваљујући паду цена набавке
- појављују се прва предузећа која почињу да се специјализовано баве пружањем услуга Интернет приступа (ИСП) грађанима
- амбијент санкција Уједињених Нација прекида међународну правну помоћ као и сарадњу полицијских органа, превасходно сарадњу са Интерполом
- законска регулатива не признаје информациони криминалитет као посебни облик криминалитета нити га санкционише

Као два најтипичнија примера могу се навести крађа износа од око 20.000 ДЕМ са рачуна кредитних картица и исплата суме у готовини преко стране банке, те ДОС напад на сервере тада најпопуларнијег интернет сајта на српском језику (www.serbiancafe.com), тј. могућности за коришћење ИПЦ-а чиме је прекинута комуникација између хиљада наших грађана како у Србији тако и у иностранству, а предузећу "ПТТ Србија - Интернет" нанесена милионска штета због прекида у пружању услуга интернет приступа.

У области борбе против високотехнолошког криминала у Србији најзначајнији помак учињен је оснивањем специјализованих органа на нивоу полиције, тужилаштва и суда. Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је ступио на правну снагу 25.јула 2005.године, основано је Посебно тужилаштво у оквиру Окружног јавног тужилаштва о Београду, посебно судско одељење у Окружном суду у

Београду и специјализована полицијска јединица при Служби за борбу против организованог криминала.¹⁸

Месна надлежност наведених специјализованих органа успостављена је на целој територији Републике Србије, док је стварна надлежност прописана чланом 3. наведеног закона и односи се на кривична дела против безбедности рачунарских података прописаних Кривичним закоником (глава 27.) као и на кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако је број ауторских дела већи од 500 или настала материјална штета прелази износ од 850 000 динара.¹⁹

Наведеним законским прописом стварна надлежност посебног тужилаштва је постављена сувише „уско“, односно да поједина кривична дела која би по својој природи требало да се налазе у надлежности специјализованог органа гоњења остају ван његовог домаћаја. Конкретно, ради се о кривичном делу приказивање порнографског материјала и искоришћавање деце за порнографију и кривичном делу фалсификовање и злоупотреба платних картица. Уколико се узму у обзир елементи починилаца ових кривичних дела и могући начини њиховог извршења - да се дистрибуција садржаја углавном врши преко Интернета као и да су прибављање релевантних идентификационих података за израду лажне платне картице, као и сама израда и коришћење, незамисливи без употребе специфичних електронских уређаја и програма који по својој природи и намени јесу рачунари и рачунарски програми - види се да је велики пропуст учињен чињеницом да се кривично гоњење учинилаца оваквих кривичних дела и даље налази у оквиру органа гоњења опште надлежности.

Решења других земаља која регулишу ову област су много строжа и воде рачуна о природи ових кривичних дела, друштвеној опасности коју

¹⁸ [3] *Кривични законик Републике Србије*, Службени гласник РС, бр.85/05, 88/05 и 107/05.

¹⁹ [4] *Закон о посебним овлашћењима ради заштите права интелектуалне својине*, Службени гласник РС, број 46/06.

представљају и заштитном објекту, при чему је и само поседовање оваквих материјала кривично дело, а као позитиван пример може се узети Норвешка чија регулатива је отишла корак даље и санкционише и само приступање Интернет сајтовима са оваквим садржајем.

6.2. Дигитална форензика у Србији

Иако је Србија међу првим земљама у своје законе уврстила и закон о високотехнолошком криминалу, још увек не постоји институција у којој је могуће обављати делатности компјутерске форензике, а и процес верификације експерата дискутабилно би могао бити решен у оквиру постојећих институција.

Све што се ради а везано је за дигиталну форензику, ради се пре свега у компанији *Data Solutions* која се налази у Београду, Крагујевцу и Новом Саду. Они раде на пољу дигиталне форнезике од 2001. године а спадају у приватне истражитељске агенције.

7. Мобилни уређаји

Мобилни уређаји су некада подразумевали искључиво мобилне телефоне, док сада обухватају читав спектар машина које се користе у свакодневном раду и животу. Од телефона, џепних рачунара, музичких *player*-а, фотоапарата, лаптоп и таблет рачунара, УСБ стикова, па све до преносивих хард дискова, све спада у мобилне уређаје. И сви су они на неки начин "smart" (паметни) уређаји и користе неки вид меморијске локације за складиштење својих података. Мобилни рачунари било кога типа, телефони, фотоапарати, музички плејери користе меморијске картице, док су УСБ и екстерни хард дискови управо то - једна врста меморије. Сви ови уређаји на овај или онај начин могу бити мета напада или се могу користити у погрешне сврхе.

7.1. Мобилни телефони

Справа која је данас смарт уређај, а ми је знамо као мобилни телефон је некад била коришћена само од стране војске и то само за разговор. Како је временом технологија напредовала, телефони су се развијали па су временом добијали додатне функције попут *SMS*-а, могућности приступа интернету, камере за сликање па потом и за снимање видео снимака, док су се данас развили јаким великом брзином и сада раде као мини рачунари и просечан, било послован или "обичан", човек не може да замисли свој дан без једног оваквог уређаја, а некад и без два.

Наравно, телефон се развио над радио фреквенцијама и први пут је инсталиран за потребе полиције 1928. године у Детроиту и то у полицијској станици јер је могао да функционише само у једном смеру (да позове све полицијске аутомобиле).²⁰

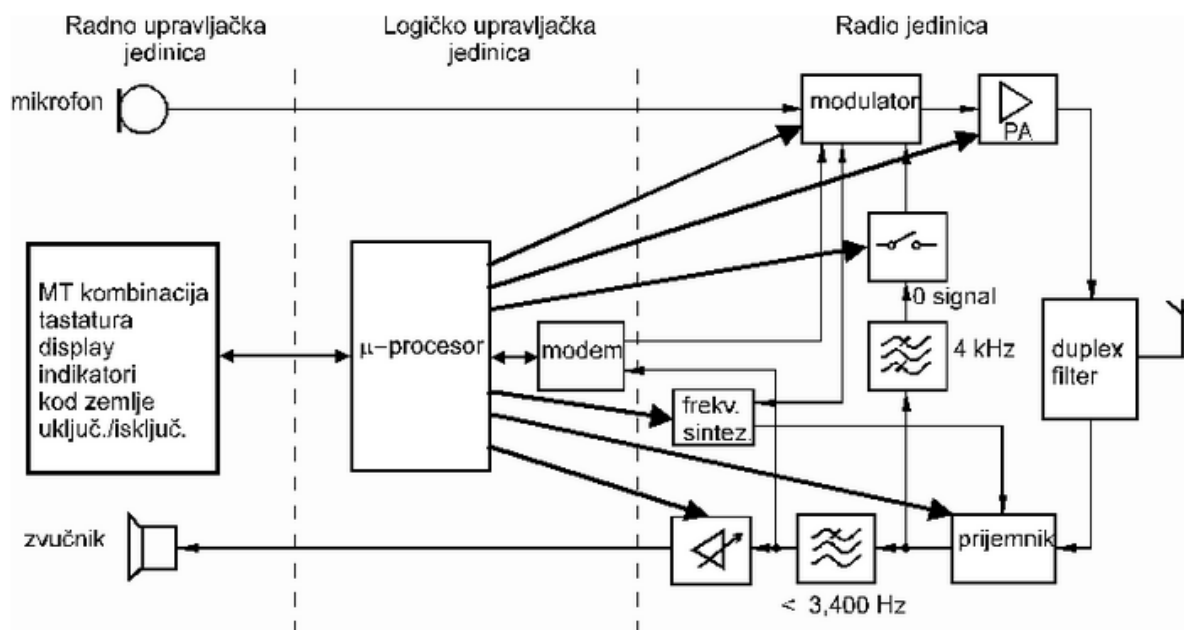
Генерацијама касније, телефон је добио одлике мини рачунара и тиме постао савршен за нападе што путем интернета, што директним контактом. Такође је и

²⁰ [17] http://sh.wikipedia.org/wiki/Mobilni_telefon (04.05.2013.)

одлично оруђе којим се злочин може извршити али и забележити многе ствари те он може бити и део доказног материјала.

Мобилни телефон можемо поделити на три јединице:

- радно управљачка јединица
- логичко управљачка јединица
- радио јединица



Слика 7.Блок шема мобилног телефона

- **Радно управљачка јединица** - Радно управљачка јединица садржи функционалне јединице које употребљава корисник. Радно управљачка јединица садржи:

- о МТ комбинацију (слушалицу)
- о дугме за укључење и искључење
- о тастатуру
- о дисплеј
- о сервисне индикаторе
- о позивни индикатор



Слика 8. *Nokia 101* - први GSM телефон

- o индикатор за роаминг аларм
- o бирач кода земље
- o сигнализатор за позив и грешку
- o посебни микрофон - звучник са могућношћу подешавања јачине звука
- o преклопку за рад без руку

- **Логичко управљачка јединица**

Велик број функција, употреба њихових комбинација, захтевала је да логика мобилног телефона буде реализована са микропроцесором. Микропроцесор даје бројне функционалне могућности као што су: *електронско закључавање, забрана бирања неких бројева, меморисање скраћених бројева* и др. Остварене су и врло важне функције:

- декодирање сигнала примљеног од МТХ и обрада примљених информација:
 - идентификација позивног канала
 - идентификација прометног канала
 - идентификација прометног подручја
 - позивање мобилног телефона
 - захтев за идентификацију
 - наредба за промену канала
 - наредба за раскидање везе

- **Радио јединица**

Радио јединица садржи одашиљач и пријемник који су спојени на заједничку антену преко дуплекс филтера. Фреквентна синтезна јединица генерише фреквенције за 168 канала. Због дуплексног рада потребно је контролни сигнал са базне станице вратити преко мобилног телефона, чиме се омогућује контрола квалитета преноса. Излазна снага одашиљача је 15 W.

Мобилни телефони нису у почетку имали меморијску локацију осим оне на СИМ картици за именик и поруке. Временом се локални капацитет телефона проширио и појавили су се телефони који су могли да надограде своју меморију уз помоћ меморијских картица различитих величина.

Мобилни телефони могу бити и средство за извршавање злочина, место злочина а и доказ.

7.2. УСБ меморија

УСБ (*Universal Serial Bus* - универзална серијска магистрала) је спољашњи прикључак намењен складиштењу података. Представља преносиви меморијски медијум. Први усб уређај је произведен од стране ИБМ-а 1998. године. Пандан је компакт дисковима и дискетама и данас се производи у разним величинама и њихов капацитет се и даље проширује, за сада је максимум 1ТВ. Базирају се на *flash* меморији која може бити *NAND* и *NOR* типа.



Слика 9. Унутрашњост УСБ стика

Разлика између НАНД и НОР типа меморије је у томе што НАНД има серијски повезане транзисторе, док су они код НОР-а паралелно повезани што утиче на перформансе те се за УСБ стикове обично користи НАНД тип флеш меморије.

УСБ уређаји могу бити помоћно средство у злочину али су обично доказ у истом.

²¹ [18] http://sr.wikipedia.org/sr/USB_memorija (04.05.2013.)

7.3. Меморијске картице²²

Меморијске картице су меморијски медијуми које користе неки други уређаји. Намењене су допуни меморије неким преносивим уређајима попут мобилних телефона, џепних рачунара, музичких плејера, фотоапарата итд.

Функционишу слично као и УСБ меморије тј. заснивају се на истом принципу: садржај се може преснимавати и чувају податке без потребе за електричном енергијом.



Слика 10. Smart Media меморијска картица

Smart Media картице су се појавиле 1995. године и одмах постале врло популарне. Тадашње картице су могле да спреме око 30 фотографија са апарата, носиле су максимум 128MB меморије. Биле су јако танке и подложне оштећењима и то више и од неких тањих модела картица. Користиле су се неколико година.

Након њих су почеле да се користе Secure Digital картице, али су се две водеће компаније, произвођачи фотоапарата и камера, Fujifilm и Olympus одлучиле за други формат картица и свету представиле xD-Picture картицу 2002. године. Оне су имале две предности



Слика 11. xD-Picture картице



Слика 12. Secure Digital картице

Нажалост, произвођачи меморијских картица нису примили нове картице као производ за масовну производњу па су оне остале релативно скупе.

Secure Digital картице су се појавиле 1999. године. Направио их је Panasonic у сарадњи са компанијом Toshiba и SanDisk и то на основу постојећег формата картица - MultiMedia Card (MMC), који је направљен две године раније од

²² [19] http://www.trustedreviews.com/opinions/how-it-works-memory-cards_Page-3 (17.05.2013.)

стране *SanDisk* - а и *Siemens* - а. Реч "*secure*" се у имену нашла јер ове картице могу да чувају и енкриповане музичке фајлове. Користе их велика већина фотоапарата, камера, мобилних телефона, џепних рачунара и музичких плејера.

Меморијске картице такође могу садржати податке о злочину или податке потребне за извршење злочина (вирусе, програме и сл.), тако да могу бити и средство и доказ о злочину јер је користе многе друге компоненте.

7.4. PDA²³

Personal digital assistant или *PDA* су џепни рачунари који су у ствари нешто слично мобилним телефонима. Сматрају се претечом паметних телефона. Скоро сви уређаји овог типа имају могућност приступа интернету, електронски екран који му омогућава да отвори *web browser*, аудио могућности које му омогућавају коришћење као преносни медија плејер, а такође их је могуће већину користити као мобилни телефон. Већина ПДА може да приступи интернету, интранет или екстранету преко *Wi-Fi* тј. *Wireless Wide Area Networks*. Већина ПДА имају имплементирану *touchscreen* технологију (поседују екране осетљиве на додир). Први ПДА је пуштен у



Слика 13. Псион 3

продају 1984. године од стране *Psion* - а, и звао се *Organizer II*. Пратио га је *Psion 3* 1991. године, који је почео да личи на ПДА стил. Он је такође имао пуну тастатуру. (Слика 13.)

Термин ПДА је први пут употребљен 7. јануара, 1992. од стране генералног директора *Apple Computer*-а *John Sculley* - ја на *Consumer Electronics*

Show-у у Лас Вегасу позивајући се на *Apple Newton* платформу за џепне рачунаре. Године 1994, *IBM* је представио први ПДА са пуном функционалношћу обичном мобилног телефона - *IBM Simon*, који се такође може сматрати првим паметним телефоном. Онда је 1996. компанија *Nokia* представила ПДА са функционалношћу мобилног телефона - *Nokia 9000*

²³ [20] <http://stevelitchfield.com/historyofpsion.htm> (14.05.2013.)

Communicator, који је постао најпродаванији ПДА на свету. Комуникатор је створио нову категорију ПДА уређаја: "ПДА телефон", која је у ствари сада категорија паметних телефона. Још један рани учесник на овом тржишту је Палм, са линијом ПДА производа који су се појавили у марту 1996.



Слика 14. Nokia 9000 Communicator

ПДА уређаји користе меморијске картице за проширење свог меморијског простора.

ПДА уређаји могу бити мета злочина због података које садрже, могу бити средство којим се злочин извршава и наравно доказ о злочину.

7.5. MP3



Слика 15. Различити iPod уређаји

Преносиви медија плејер (*Portable Media Player (PMP)*) је уређај који се користи за складиштење и "пуштање" дигиталних материјала попут музике, фотографија, видео снимака, докумената итд. Ова врста уређаја за складиштење материјала обично користе микро-дискове, флеш меморије или меморијске картице. Пандан овоме су аналогни уређаји који читају касетне траке или плоче тј. компакт дискове. Добили су назив *MP3 плејери* јер се продају под уређаје који само пуштају музичке фајлове, док они подржавају и друге формате. Претече плејера су *Portable CD player* а још пре њега и *Personal*

stereo. Један од првих дигиталних аудио плејера је направљен 1979. године од стране британског научника Кане Крамера (*Kane Kramer*, 23.04.1956.) и звао се *IXI*. Овај прототип је могао да пушта аудио материјал око сат времена. Нажалост, овај патент није заживео толико да почне масовно да се производи. Након тог патента, Крамер се запослио као саветник у компанији *Apple* која је произвела *iPod* који је постао светски хит од првог појављивања 2001.године. Његова прва генерација је имала 5GB меморије и заснивала се на *Toshiba* хард диску. Одмах следеће године је изашла у продају и друга, побољшана генерација.

Преносиви музички уређаји могу да се користе као преносива меморија па могу бити средство за извршавање злочина, такође је често и доказ.

8. Заштита мобилних уређаја

Како се данас технологија све већом брзином развија, истом брзином се развијају начини на који се технологија може користити у погрешне сврхе. Најважније је заштитити се адекватно од напада било које врсте, уколико је то могуће. Често је за просечног корисника то немогуће.

8.1. Заштита мобилних телефона²⁴

Поверљивост података, интегритет и аутентикација идентитета су три најпожељније безбедносне функције на смарт телефонима.

Већина смарт телефона подржава синхронизацију између уређаја и персоналног рачунара. Ова функција омогућава да други корисник приступи систему датотека смарт телефона. Дакле, да би поверљиви подаци остали поверљиви, корисници треба да користе технике кодирања и да избегавају складиштење осетљивих информација у *plaintext* - у (отвореном тексту) на смарт телефону. Интегритет се односи и на податке и на систем. Продавнице апликација треба да потврде интеграцију софтвера који се налази на продавници, да би се избегла злонамерна модификација. Паметни телефони би

²⁴ [8] Yong Wang, Kevin Streff, Sonell Raman, *Smartphone Security Challenges*, 2012.

треба да обезбеде механизме за заштиту интегритета система. Они такође треба да блокирају неовлашћене захтеве за приступ подацима.

Систем аутентикације смарт телефона може да заштити његове кориснике од злонамерних напада којима се краду бројеви телефона и ММС порука (мултимедијална порука). Из разлога што фемто-ћелије (*femtocells*²⁵) побољшавају покривеност и капацитет, аутентикација постаје веома важна ради потврде идентитета пошиљаоца.

Смарт телефони треба да одвоје осетљиве податаке од неосетљивих и да корисницима омогуће флексибилност описивања података као осетљивим. Иако осетљиви подаци могу бити лака мета за хакере, уколико имамо јасно дефинисане осетљиве податке биће их лакше заштити јер их има мање уместо да се штите и можда небитни подаци. Осим тога, једноставне технике безбедности, као што су шифровање и стеганографија²⁶, могу да заштите осетљиве податке. Изолација осетљивих података је такође добра за пословање. Корисници смарт телефона могу да идентификују корпоративне податаке као осетљиве и да им доделе виши ниво безбедности.

Поред криптовања осетљивих података ускладиштених у смарт телефона, корисници треба да шифрују своје меморијске картице. Без одговарајућег кључа за дешифровање, смарт телефон не би требало да приказује закључани садржај меморијске картице. Међутим, криптографија јавним кључем, као што је RSA, обично захтева додатну рачунарску снагу и треба да се користи са опрезом да не би дошло до пражњења батерије.

Миграцију података са паметних телефона на облак (*Cloud*) је још један начин да се заштите осетљиви подаци. Детекција упада заснована на облаку може помоћи у откривању злоупотребе и може да заштити осетљиве податке. Ова опција ће укључити трошкове за сервис облака који је још увек у строго комерцијалној фази.

²⁵Базна станица за мобилне телефоне, мале снаге и димензија.

²⁶Дисциплина која се бави сакривањем поверљивих информација у оквиру неких других, свима доступних информација.

Многа предузећа су почела да истражују могућности за решење безбедносних проблема за смарт телефоне. Тренутно су корисници смарт телефона искључиво сами одговорни за инсталирање апликација и о њиховој безбедности. Међутим, безбедност захтева сарадњу међу корисницима мобилних телефона, пружаоца услуга, и партнера. Безбедност паметних телефона је изазов и компликована акција. Постоји неколико једноставних начина да се побољша безбедност смарт телефона:

- Подизање свести о безбедности. Као и десктоп или лаптоп рачунар, смарт телефон може бити хакован или заражен. Корисници смарт телефона треба да буду свесни претњи и могућих напада приликом инсталирања софтвера или давања дозволе за приступ флеш меморији или сензору.
- Подесити лозинку и *auto-lock* (аутоматско закључавање) након одређеног временског периода. Већина смарт телефон подржава ове заштитне функције.
- Не треба држати незаменљиве и јединствене податке у смарт телефону пошто се могу лако изгубити или украсти.
- Неопходно је редовно радити *back-up* телефона. Синхронизовати телефон са рачунаром и увек имати резервну копију података.
- Потребно је *Bluetooth* искључивати након употребе. Вируси се шире преко *Bluetooth* -а на паметном телефону.
- Избегавати несигурне *Wi-Fi* приступне тачке за повезивање на Интернет. *Packet sniffer* софтвер као што је *Wireshark* могу да открију корисне информације податковног саобраћаја из смарт телефона.

Неки суптилни знаци могу да указују на то да је паметни телефон под нападом:

- Батерија телефона је топла чак и када се уређај не користи
- Телефон светли изненада и насумично, чак и када се не користи
- Неочекивано се чују „бип“ или клик звуци у телефонским разговорима.

8.2. Заштита флеш меморије

Већина корисника који за пренос података користе УСБ флеш не размишља много о сигурности података који су снимљени на њему. Ипак има оних којима је сигурност на првом месту. У употреби је више различитих решења која механички штите флеш дискове и меморијске картице.

Произвођачи у својој понуди имају решења и за оне који не желе да подаци који су снимљени на УСБ флешу дођу у погрешне руке. Некада се све сводило само на прекидач којим би се забранио упис, али због његове бескорисности престало са производњом таквих решења. Најновија решења пружају 256 битну хардверску енкрипцију података. Неретко је могуће чак и креирати вишеструка заштићена подручја која су заштићена посебном лозинком или отиском прста на скупљим уређајима. Подаци се у та подручја могу једноставно копирати и биће аутоматски криптовани у „лету“. Као додаток уграђена томе, у многе, је уграђена *File Shredder*²⁷ функција која уклања све трагове обрисаних података. На тај начин није их више могуће реконструирати посебним форензичким програмима већ су обрисани заувек. До сада су били подржани искључиво *Windows* системи, а сада и *Mac* корисници могу искористити могућности које нуде драјвови са повишеним степеном безбедности података.

Осим хардверских постоје и многа софтверска решења као што је *USB Lock AP*²⁸ компаније *Advanced Systems International* који пребацивањем само 3 фајла на УСБ диск омогућава исте функционалности као и хардверска заштита. У случају да се жели потпуна забрана рада са УСБ меморијама малом изменом у *Windows registry* бази може се омогућити неометан рад осталих УСБ уређаја, који се прикључују на рачунар, а забранити коришћење флеш дискова.



Слика 16. *USB Lock AP*

²⁷ [21] <http://saveti.kombib.rs/sigurnost-podataka-na-usb-flash-memoriji.html> (14.05.2013.)

²⁸ [22] <http://www.advansysperu.com/usb-lock-standard.html> (17.05.2013.)

9. Дигитална форензика у функцији заштите

9.1. Форензика мобилних уређаја

Циљ форензике мобилних уређаја је рекуперација дигиталних података, тј. доказа с мобилног уређаја разним методама. Свака метода која се користи садржи одређене услове, чијим се испуњавањем решава проблем ваљаности сакупљених података. На тај начин сакупљени подаци се могу користити као докази у судским поступцима као и у многим другим процесима. Из праксе је статистички показано да постоји велики број случајева где је таква врста доказа била кључна.

Форензика мобилних уређаја се разликује од форензике десктоп рачунара јер мобилни уређаји делују под разним мрежама и то утиче на процесе пристизања, чувања и обраде података. Осим прикупљања података, мобилна форензика придаје значај и вези између процеса прикупљања података и хардвера уређаја. На тај начин кориснику се даје повратна информација која даје потпуни увид у организацију мобилног уређаја и спектар његових могућности. Сви поступци раде се корак по корак што даје додатну сигурност ваљаности излазних резултата.

9.2. Прикупљање доказа са мобилних уређаја

Начини на који се докази прикупљају са мобилних уређаја се могу разликовати у зависности од тога који је уређај у питању и у каквом је стању, чак и у каквом су стању подаци који се прибављају.

Форензика мобилних уређаја која спада под компјутерску форензику покрива мобилне телефоне, смарт телефоне, таблете, личне дигиталне помоћнике (*PDA*), и GPS - пријемнике је област под компјутерском форензиком. С обзиром да су мобилни уређаји све више инструмент, мета, или запис кривичног дела, они су од интереса за кривичну истрагу, грађанске парнице, и прикупљање обавештајних података. Неки тврде да мобилни уређаји садрже више доказа по бајту од традиционалних рачунара. Пошто већина смарт телефона сада долази са софистицираним апликацијама, уграђеним камерама, пуно складишног

капацитета, и брзим мрежним конекцијама, огромна количина рачунарске снаге је лако доступна корисницима. Иако форензика мобилних уређаја подразумева проналажење и испитивање података чак и ако су они можда избрисани, и за кривичне и за грађанске поступке, процеси и средства се такође користе у апликацијама изван суднице. Подаци који се могу извући из ових уређаја укључују историју позива, послатих и примљених кратких порука (СМС) и мултимедијалних порука (ММС), контакте и бројеве телефона, електронску пошту, фотографије, видео снимке, географске и ГПС информације, подешавања бежичне мреже, *web* историју прегледања, гласовне поруке, информације са друштвених мрежа, историје апликација и лог фајлове, и друге податке који се могу наћи уз помоћ смарт апликација.

Бројни комерцијални и *open source* производи су доступни за прикупљање и анализу података из мобилних уређаја, од пакета програма везаних за камеру који узимају "слику" - *screenshot* екрана, до производа који анализирају базу података и хардвер да би физички испитали чипове уређаја.



Слика 17. Производи који се користе - 1) *Cellebrite UFED*, 2) *Micro Systemation XRY*²⁹

Форензика мобилних уређаја захтева процесе и алате који могу извући информације од најмање шест различитих мобилних оперативних система,

²⁹ [8] Yong Wang, Kevin Streff, Sonell Raman, *Smartphone Security Challenges*, 2012.

укључујући *iOS*, *Android*, *Windows Mobile*, и још хиљаде модела телефона, таблета и ГПС уређаја.

Чак и ако форензичар може доћи до физичке меморије уређаја, испитивање тог бинарног складишта можда захтева старомодну анализу са хекс едиторима (*hex editors*³⁰), стандардне алате компјутерске форензике и анализу регуларним изразима. Нпр., Андроид телефони имају значајне фрагментације и варијације верзија оперативног система, што чини лоцирање заједничких података оперативних система и уређаја тешким, чак и *Apple iPhone* даје различите податке у зависности од верзије оперативног система и од тога да ли је телефон *jail-broken* (ослобођен од ограничења наметнутих од стране компаније *Apple* - откључан).

Многи "глупи" Таблети на тржишту складиште контакте и СМС податке/поруке на СИМ картици, док слике или видео снимке чувају локално на уређају. Таблете се понашају исто као и телефони, што се тиче прикупљања форензичких података. Због невероватне количине личних и пословних података који се налазе на мобилним уређајима, или се могу извести из информација са уређаја, безбедност и приватност ових уређаја су изазов.

Осим стављања информација о кориснику на телефон, оперативни систем такође складишти информације без знања корисника. Нпр., у априлу 2011. године, *Apple* је добио велику медијску пажњу када је постало познато да је *iPhone* бележио детаљну историју о географским локацијама корисника и то у облику незаштићене датотеке. Једноставном екстракцијом, форензичар може да створи гео карту свих места које је *iPhone* тј његов корисник посетио. Кључна лекција: осетљиви подаци би требали бити кодирани у смарт телефонима.

УСБ и меморијске картице имају неколико одлика по којим се разликују од стандардних меморијских уређаја. Осим карактеристика, као што су физичка величина, начин рада и сл.

³⁰ нпр.: *HxD Hex Editor*

За разлику од хард дискова који се најчешће налазе у унутрашњости рачунара и који су, у већини случајева, извори искључиво дигиталних доказа, преносиве меморије на себи имају и бројне отиске прстију, јер се чешће преносе „из руке у руку“, а и лако је утврдити ко је задњи имао у рукама ту меморију. Веома је битно руковање са овим уређајима и узимање свих врста физичких доказа пре саме дигиталне форензике. Чак и ситна физичка оштећења на конекторима могу бити доказ који ће осудити или ослободити осумњиченог.

У свету је познато више случајева доказивања умешаности у криминалне радње повезане са дечијом порнографијом, када је као доказ прихваћен налаз форензичара који су на основу ситних (микроскопских) оштећења на меморијској картици утврдили да су коришћене у одређеном фотографском апарату. Наиме распоред конектора, начин убацивања и место на коме се меморијска картица налази, остављају на картици различита оштећења, макар се радило и о два апарата из исте серије.

У случају да је потребно прикупити податке над оштећеним меморијама које се заснивају на флеш типу, или обрисаним подацима треба извршити следеће:

- Одвојити меморијски чип од оштећеног уређаја
- Прочитати све секторе меморије и креирати идентичну “слику” меморије
- Детектовани одређени микс страна меморије
- Отклонити микс
- Применом адекватног алгоритма све странице спојити у једну целину

Након овог процеса могућ је логички приступ подацима. Односно, неопходно је одредити параметре примењеног фајл система (90% случајева *FAT12*) и након тога рестаурирати логичку структуру и копирати податке. Изузеци од описаног поступка постоје. Мини и микро СД картице не поседују контролер, а неки уређаји имају енкриповане стране у оквиру меморија које је немогуће дешифровати у случају отказа контролера. Подаци се на меморије смештају потпуно другачије него у хард дисковима. Целокупна меморија је подељена на

"стране", величина стране као и начин смештања зависи од типа алгоритма који је примењен. Такође распоред страна у оквиру саме меморије није линеаран, у зависности од типа примењеног алгоритма постоји више могућих варијанти микса самих страна.³¹

Што се тиче форензике личних дигиталних помоћника (*PDA*), процес прикупљања форензичких информација са ових уређаја је сличан процесу прикупљања података са других сличних уређаја. У основи се састоји из четири основна корака:

- испитивање
- идентификација
- прикупљање
- документовање

На овим корацима се у принципу заснива било која форензичка истрага уређаја различитих типова.

Пре свега је потребно идентификовати изворе доказа, у овом случају то могу бити уређај, његово кућиште, извор енергије или било који спољашњи уређај са којим је ПДА имао додир или био синхронизован са њим. Након прикупљања доказа са спољашњег кућишта уређаја потребно је испитати уређај "изнутра" тј.обрадити његове меморијске локације и оперативни систем, као што је већ раније описано код смарт телефона.

Музички преносиви уређаји се обрађују слично као обични "тврди" дискови рачунара због своје природе система. Као што је пракса код персоналних рачунара, и код форензике ових уређаја потребно је направити "слику" система (*image*) јер није препоручљиво радити са оригиналним подацима. Да би се очувао интегритет података, форензичари користе "*hash*" као отисак података који ће да гарантује да подаци нису мењани ни у једном кораку прављења *image-a*.³²

³¹[23] <http://www.datasolutions.rs/srp/spasavanje-podataka/spasavanje-podataka-sa-digitalnih-medija.html> (25.05.2013.)

³² [1] Anthony Reyes, Jacki Wiles, *The Best Damn Cybercrime and Digital Forensics Book Period*, 2007.

9.3. Алати за прикупљање доказа

Алати који се користе за прибављање форензичких података са мобилних уређаја зависе од тога који је уређај у питању и за сродне уређаје се користе исти алати.

Неки од најпознатијих алата који се користе за прикупљање података са мобилних телефона, *GPS* уређаја и таблет рачунара су³³:

- *Cellebrite Universal Forensics Extraction Device (UFED)*
- *Oxygen Forensic Suite 2012*
- *Paraben Device Seizure*
- *MicroSystemation XRY*
- *Logicube CellDEK*

Наведени алати користе исте протоколе као и нефорензички алати произвођача, али не имплементирају команде које експлицитно модификују садржај меморије мобилног телефона. Мобилне телефоне, *GPS* уређаје и таблет рачунаре обједињује то што се заснивају на истом оперативном систему па се прикупљање података са њих обавља на сличан начин. Произвођачи непрестано прате развој нових модела и своју базу непрестано допуњују новим моделима који се појављују на тржишту.

Што се тиче *PDA* уређаја, не постоји велики број алата који могу да се користе за форензичку истрагу ових уређаја. Најраспрострањенији су *PDA Secure*, *PDA Seizure*, *EnCase*.

PDA Secure нуди побољшану заштиту лозинком заједно са енкрипцијом, уређај за закључавање, и брисање података. Омогућава администратору бољу контролу како се уређаји користе у мрежама. Осим тога, омогућава подешавање времена и периода праћења информација као што су логовања на мрежу, инфрацрвени пренос, и све апликације које су се тада користиле.

PDA Seizure је свеобухватан алат који помаже у "заузимања" уређаја. Ради у *Windows* окружењу и може издвојити радну меморију (*RAM*) и сталну меморија

³³ [24] <http://igorfranc.blogspot.com/2012/11/digitalna-forenzika-mobilnih-telefona-i.html> (29.05.2013.)

(ROM). Има графички кориснички интерфејс (GUI) који је лак за коришћење, и укључује алате који су потребни за истраживање датотека који се налазе у уређају. Подржава различите платформе на којима форензичар може да добије и да испита информације на уређајима и за *Pocket PC* и за *Palm* оперативни систем.

За анализу музичких уређаја се могу користити било који алати који могу да раде са *FAT32* системима, тј. било који алат који се користи за форензичко прикупљање података персоналних рачунара: *Guidance Software's EnCase*, *AccessData's FTK*, *Brian Carrier's Sleuth Kit*, *Paraben's P2*, итд.³⁴

10. Пример прикупљања података са мобилног телефона

Форензика мобилних телефона може да се подели на форензику меморијске локације и на форензику СИМ картице. У току процеса прикупљања података са СИМ картице може се десити да је потребан *PIN* (Personal Identification Number) код.

Разликујемо две врсте приступа аквизицији података са мобилних телефона:³⁵

1. **Аквизиција на логичком нивоу** је прикупљање података са меморије мобилног телефона коришћењем система датотека, односно оперативног система телефона. Да би се на овај начин прикупљали докази, потребно је познавати сваки телефон са којим се ради, да би се број погрешних корака свео на минимум (пре свега се мисли на кораке који би вршили промене на телефону). Због тога СМС поруке, које су врло занимљиве за форензичку анализу, уједно представљају изузетно захтеван сегмент мануелне аквизиције, јер се у извештај мора унети цео непромењен садржај сваке поруке. Пошто се, због природе савременог организованог криминала, често од страних држављана привремено одузимају мобилни

³⁴ [1] Anthony Reyes, Jacki Wiles, *The Best Damn Cybercrime and Digital Forensics Book Period*, 2007.

³⁵ [26] http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic.html (05.06.2013.)

телефони који садрже велики број порука на матерњем језику власника, процес аквизиције се додатно пролонгира.

Апликације на телефонима не теже систематичном приказу свих података који би били занимљиви форензичарима, па се најчешће троши доста времена на претраживање различитих менија и подменија. Пример опет могу бити СМС поруке, до чијих се детаља везаних за саму комуникацију, као што су датум, време и претплатнички број пошиљаоца, долази путем подменија, јер екран који приказује садржај поруке најчешће приказује само назив из телефонског именика). Мануелном прегледу се приступа само ако се тражи одређени дигитални доказ на уређају, или ако не постоји други начин да се приступи мобилном телефону и прикупе докази.³⁶ Посебан изазов су јефтини, а нови модели мобилних телефона које продају оператори, који често немају ниједан интерфејс за комуникацију са уређајем, али имају велике капацитете за складиштење СМС порука. Евентуалне промене које могу настати (на пример, примање позива и СМС порука) услед потребе да у току мануелне аквизиције уређај буде укључен спречавају се коришћењем Фарадејевог кавеза (најчешће у облику специјалних кеса које блокирају електрично поље) и клонирањем СИМ картица;

2. **Аквизиција на физичком нивоу** представља копирање целокупне меморије, бит по бит, што омогућава прикупљање и података из простора који није лоциран од стране оперативног система, односно опоравак обрисаних података. Аквизиција путем конекционих сервиса представља тренутно најзаступљенију методу, на којој су базирани форензички алати који користе протоколе за слање команди и пријем података за комуникацију са сервисима. Користе се било отворени протоколи као што су *AT Command Set*, *SyncML* или *OBEX*, који су већ застарели, или фабрички протоколи попут *Nokia FBUS*. Постоје и развојни алати који програмерима омогућавају креирање апликација које користе сервисе мобилних телефона без имплементације основних протокола. Аквизиција преко конекционих сервиса врши се помоћу две врсте алата.

³⁶ [9] Casey, E., *Digital evidence and computer crime: forensic science, computers, and the Internet*, 2004.

Најчешћи се користе алати самих произвођача мобилних телефона или независних програмера, који омогућавају прикупљање одређеног скупа података, а намењени су пре свега синхронизацији рачунара и мобилног телефона или прављењу резервних копија, а не форензици. Честа последица непажње при коришћењу оваквих алата је озбиљно нарушавања очуваности дигиталних доказа, а добијени подаци су углавном у форми неупотребљивој за креирање извештаја (чести су били проблеми са *Nokia PC Suite* (за различите моделе овог произвођача), који СМС поруке приказује табеларно, али не дозвољава копирање података, нити нуди било какав експорт). У другу врсту форензичких алата спадају већ споменути форензички алати за прикупљање информација.

Наведени приступи се примењују применом различитих метода аквизиције података са мобилних телефона:

- *Конекциони агенти* су мали програми (на пример, конекциони агент форензичког алата ХРУ инсталиран на телефону *Nokia N95* заузима свега 34kb) који се смештају на циљни уређај да би обезбедили конекцију и размену података између телефона и форензичког алата. Овакав приступ користи клијент-сервер архитектуру са агентом у улози сервера, без кога алат не би могао да дође до података из меморије мобилног телефона. Пошто агент игра улогу конекционог сервиса, аквизиција података је у суштини слична претходно описаној. Метода се често користи код паметних телефона, а главни проблем је што, коликогод његов софтвер био мали, агент мора бити смештен у меморију, чиме се њен садржај мења.

- *Директан приступ меморији* мобилног телефона је највише усклађен са форензичким принципима, али представља и најзахтевнију методу аквизиције података.³⁷ Ова метода прикупља податке на физичком нивоу и омогућава прављење форензичке копије целе меморије мобилног телефона, без обзира на то колики меморијски простор је заузет. Директан приступ меморији омогућава опоравак обрисаних или делимично истиснутих уноса, као и заобилажење

³⁷ [10] Willassen S., *Forensic analysis of mobile phone internal memory*, 2005.

безбедносних мера које би иначе онемогућиле приступ подацима на логичком нивоу и пред којима су остале методе аквизиције немоћне без интервенција чији је утицај на очуваност дигиталних доказа неизвештан.Још једна предност директног приступа је његова независност од тога да ли ће оперативни систем мобилног телефона обезбедити исправне резултате аквизиције, што није случај са осталим методама. Могу се применити три методе директног приступа³⁸:

- уклањање меморијског чипа са штампане плоче мобилног телефона и читање његовог садржаја (ово је за кривични поступак можда исувише ризична процедура, јер чип може лако да буде уништен температуром која се користи за његово одвајање од плоче, а самим тим и потенцијални дигитални докази);
- употреба порта за JTAG тест (*Joint Test Action Group*, стандардизована процедура за тестирање интерконекија на штампаној плочи и подблокова унутар интегрисаног кола³⁹) ради прављења комплетне форензичке копије садржаја променљиве и непроменљиве меморије телефона. Недостатак је што је на новијим моделима све теже наћи порт, односно доћи до њега, пошто га произвођачи често крију;
- употреба алата за флешовање (*flasher tools*) намењених за програмирање меморије уређаја (EEPROM или флеш меморије), или за откривање грешака и дијагностику, за шта их произвођачи често користе. Проблем код примене ове врсте алата је што у одређеним случајевима могу да прочитају само део меморије, а уз то сваки произвођач има свој, другачији, интерфејс за приступ, па је немогуће постићи свеобухватну применљивост.

Примена било које од три наведене методе директног приступа захтева висок ниво техничке обучености и знања, као и лабораторијске услове за рад.Највећи недостатак у односу на остале методе је што се посао не завршава аквизицијом, јер је неопходно анализирати сирове податке и из њих издвојити

³⁸[11] Keonwoo Kim, Dowon Hong, Kyoil Chung, Jae-Cheol Ryou, *Data Acquisition from Cell Phone using Logical Approach*, 2007.

³⁹ [25] http://en.wikipedia.org/wiki/Boundary_scan

смислене и употребљиве информације, односно доказе, који ће моћи да буду презентовани у разумљивој форми.⁴⁰

- *Прикупљање података из GSM мреже.* На овај начин се, пре свега, могу сазнати детаљни подаци о оствареним комуникацијама уређаја за дужи временски период, а који су при том много поузданији него они који се чувају на самом телефону, па се често ова метода аквизиције користи за валидацију података прикупљених неком другом методом. Може се закључити да не постоји идеалан метод аквизиције података, већ мора да се направи компромис између ефективности и ефикасности, односно да се на основу оперативних података одреди приоритет и изабере одговарајућа метода за сваки случај понаособ. Савремени форензички алати обједињују више метода и приступа, уз настојање да врше што мање измене на телефону, а да прикупе што више дигиталних доказа. У циљу доказивања да својим акцијама није нарушило очуваност дигиталних доказа, лице које врши аквизицију мора да документује све активности у раду са мобилним телефоном и да интеракцију са уређајем сведе на минимум. Што је више интеракција, то је компликованије доказати да акције нису компромитовале дигиталне доказе⁴¹. Уколико је мобилни телефон приликом привременог одузимања стављен у омот и запечаћен а бранилац или окривљени присуствује уклањању омота и извођењу аквизиције, остварени су сви услови да се тако прикупљени подаци могу користити као дигитални докази, односно отклоњене су сумње у евентуално нарушавање доказног материјала.

Micro Systemation XRY 5.1.⁴²

Алат за аквизицију података са мобилних телефона, ГПС уређаја и таблет рачунара, погодан је за оба типа аквизиције (физичка и логичка). Базира се на *Wizardu* који корисника води кроз цео процес прикупљања података. Све екстракције, било логичке или физичке се чувају у *XRY* фајлу који остаје у свом природном облику због сигурности. Из овог фајла се даље могу изводити

⁴⁰ [26] http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic.html (06.05.2013.)

⁴¹ [13] Mokhonoana P., Olivier M., *Acquisition of a Symbian smart phone's content with an on-phone forensic tool*, September 2007.

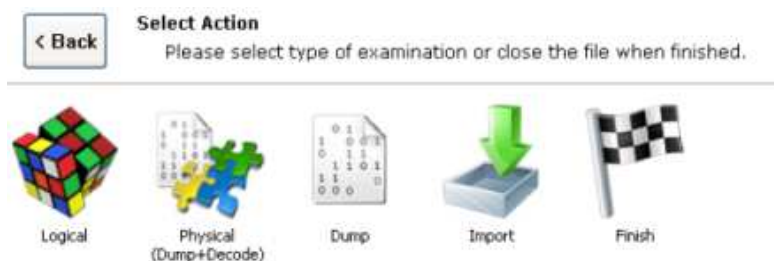
⁴² [27] <https://viaforensics.com/resources/white-papers/iphone-forensics/micro-systemation-xry/#forensic-acquisition> (10.06.2013.)

извештаји који се могу приказати у *Word*, *Excel*, *Open Office* или *PDF* формату. Могу се бирати докази који ће бити, или неће бити, у извештају. Такође постоји и читач који омогућава трећој страни да се укључи у коментарисање извештаја али да се одржи интегритет података. Последња верзија програма је лансирана 28.06.2010. године и чак може да чита и *Apple iPad*.



Слика 18. *Micro Systemation XRY*

Када покренемо алат треба да одаберемо који начин аквизиције хоћемо - логичку или физичку. Алат покрећемо када смо на кабал прикачили неки мобилни уређај - у овом примеру је то мобилни телефон *Apple iPhone3G*.



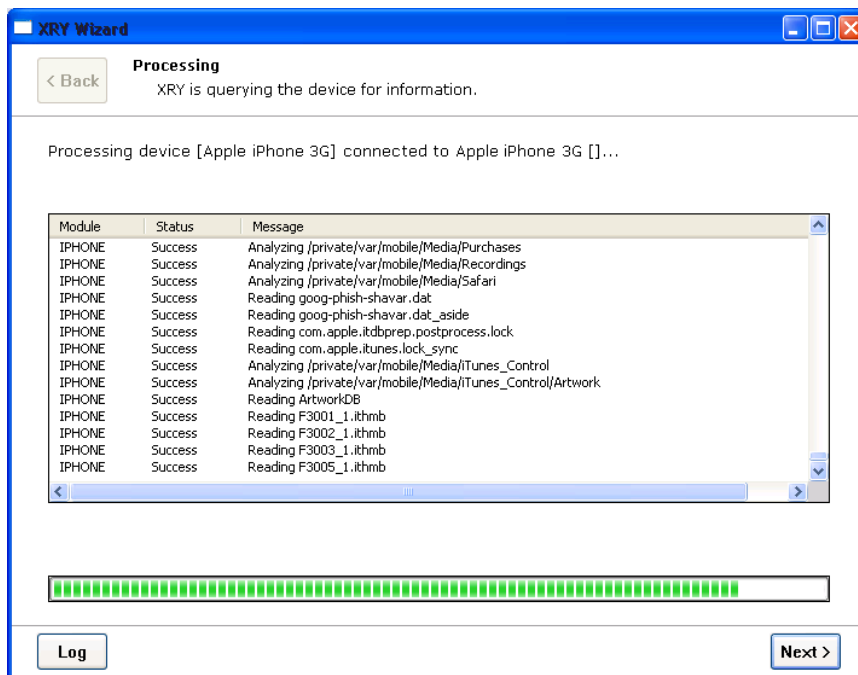
Слика 19. Тип аквизиције података

У овом случају је одабрана логичка аквизиција и приказује се следећи прозор:



Слика 20. Логичка аквизиција

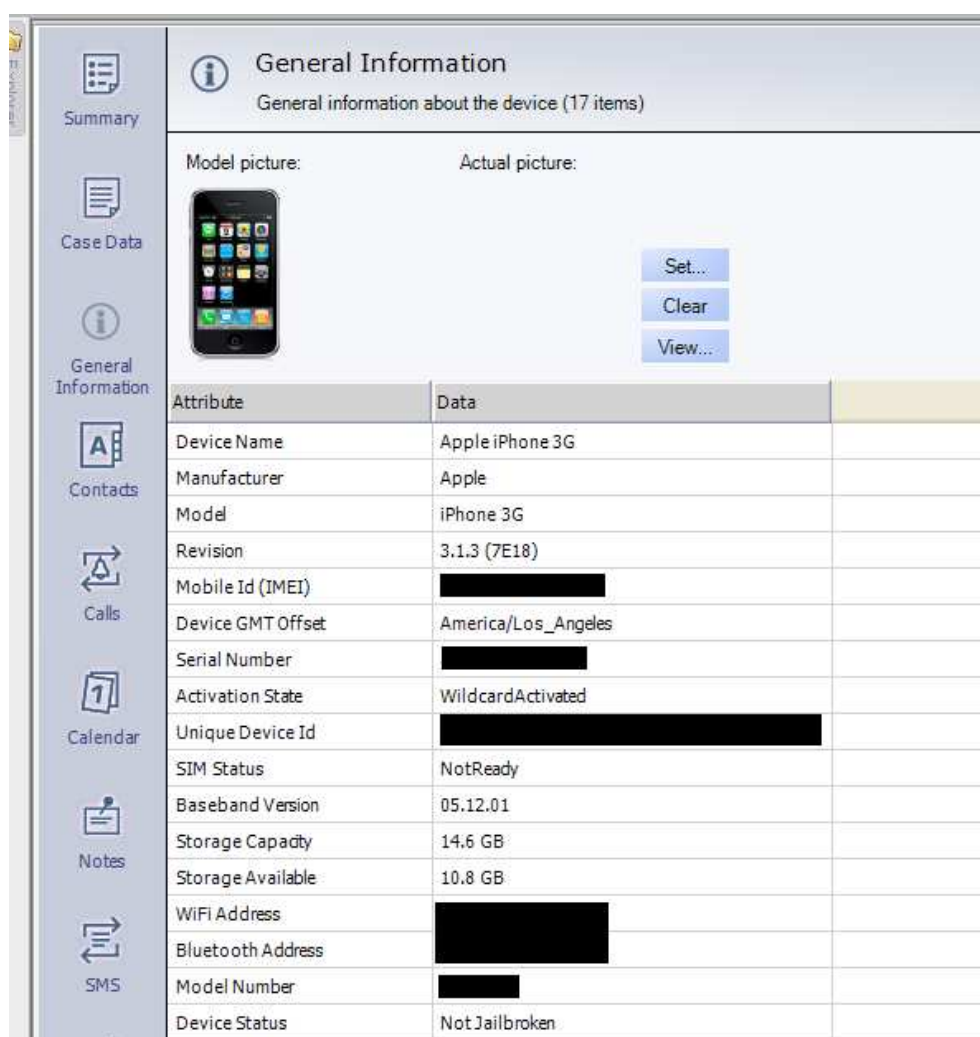
На слици 20. су приказане све врсте података које ће бити прикупљене овим алатом за овај уређај. Ово може да варира у зависности од уређаја. Кликом на *Next* започиње се процес прикупљања података који за овај уређај траје око 30 минута.



Слика 21. Процес прикупљања података

Када се скенирање и прикупљање података заврши, све се чува у ".xry" фајлу који када га отворимо приказује резултате извештаја, а са леве стране приказује стабло података са следећим категоријама: *Summary, Case Data, General Information, Contacts, Calls, Calendar, Notes, SMS, MMS, Pictures, Videos, Audio, Documents, Files, Log*. У категоријама СМС, ММС, позиви и говорна пошта постоји колона "Deleted" на крају сваког реда где се налазе обрисани подаци.

Кликом на *General Information* се добија следећи прозор где се виде основне карактеристике о уређају:



Слика 22. *General Information*

Одабиром различитих категорија мењају се приказани подаци. О контактима се приказују све информације, посебно за појединачно одабране контакте на десној страни прозора. Позиви изгледају слично као дневник на телефону,

приказују пропуштене, примљене и одлазне позиве. Овај алат је један од ретких који приказује обрисане белешке као и било које друге прочитане са уређаја, остали алати креирају прилично нејасан фајл.

Notes				
Notes stored in the device (3 items)				
Summary	Text	Created	Deleted	Deleted Info
☐ Check on loans	Check on loans	2010-05-19 01:36:55 (UTC)		
☐			Yes	wkPick up prescription
☐			Yes	Pick up prescription

Deleted Info: Pick up prescription

Deleted: Yes

Слика 23. Белешке

СМС поруке се са телефона преузму са свим могућим детаљима.

SMS		
SMS messages sent or received from the device (46 items)		
Number	Name	Message
☒ 1 (312) [REDACTED]		Got USBs connected to vm!
☐ (312) [REDACTED]	[Andrew Hoog]	Got USBs connected to vm!
☐ (219) [REDACTED]		Are you watching biggest loser?
☐ (219) [REDACTED]		When do theblackhawks start

Number: 1 (312) [REDACTED]

Message: Got USBs connected to vm!

Time: 2010-05-18 22:54:28 (UTC)

Status: Sent

Storage: Device

Index: 1

Folder: Sentbox

Слика 24. СМС поруке

ММС поруке се сачувају или могу директно из софтвера да се покрену. Сlike и видео снимци се такође налазе у засебним категоријама и садрже све податке икад снимљене са овим апаратом, чак и оне које су послате преко ММС порука.

Подаци који су за мало напредније кориснике, тј. подаци који су можда битнији за истрагу се налазе у лог секцији. Ту се могу наћи подаци о приступима мрежама, историјат претраге интернета, обележивачи, претраге, налози итд.

Сваки податак у овом алату има свој индексни број и "кућицу" која може да се чекира да би се податак приказао, или не приказао, у коначном извештају.

11. Сценарио – форензика мобилног телефона осумњиченог

Компанија **WBS - World Bank Society**, као водећа банка намењена младим амбициозним људима који су поред осталих услуга које нуди једна банка спремни да пробају нове технологије у служби банкарства. Ова банка даје могућност својим клијентима да све своје послове обављају путем електронских уређаја попут личних рачунара, мобилних „паметних“ телефона и таблета. У то спадају услуге плаћања, мењачки послови и пренос новца између локалних рачуна, што се може обавити путем телефона. Сваки клијент је 100% сигуран, као и његов новац и сваки клијент има свог личног банкара. Банкари су такође млади образовани људи који су ту за клијенте 24 сата дневно, 7 дана у недељи. Приликом запошљавања банкара спроведен је велики број тестова како би се будући запослени проверили јер треба да обављају веома озбиљан посао. Сваки клијент има могућност да позове свог банкара и да му путем позива упути захтев за неку банкарску услугу у смислу плаћања или преноса новца. Циљ је да се клијенти растерете од непотребних процедура и да пре свега послују сигурно.

Нажалост, сигурност овог типа пословања је угрожена једним немилим догађајем. Наиме, неколицина клијената је открила минималне а честе одливе новца са њихових рачуна у непознатом правцу. Детаљном истрагом полиције, која је одмах позвана да интервенише, изведени су следећи закључци:

- сви клијенти су губили мале, скоро не приметне своте новца приликом сваке нормалне трансакције, што се на крају месеца јасно види
- сав нестали новац је одлазио наводно на разне таксе и провизије које су износиле од 1 до 20% од сваке трансакције, у зависности од обима трансакције
- све трансакције овог типа су се одигравале кад год је клијент вршио неку банкарску услугу преко свог личног банкара

- све трансакције је вршио **исти човек!**

Тужба: Лице Јован Слобеновић, старости 25 година, са пребивалиштем у Београду је оптужено за **проневеру новца** и за **крађу бројева рачуна и приступних података налозима електронског банкарства** клијената фирме у којој је лице запослено. Сумња се да је лице проневерило више од 100.000 еура, што у датој валути, што у динарској противвредности, приликом сваке трансакције клијената. Сумња се да је лице након сваке трансакције коју је извршио за сваког свог клијента, одређену количину новца пребацивало на посебан рачун фирме која је престала да постоји, где се тај новац даље преносио, вероватно на његов лични рачун. Поверљивост клијент – банкар је нарушена. У случају да се кривица докаже, лицу следује затворска казна од 2 до 10 година затвора уз услов да се новац врати. Уколико није у могућности да врати новац, казна ће се продужити или додатном затворском казном или друштвено корисним радом. Против Ј.С.-а је подигнута тужба од стране свих клијената који су му били додељени.

Мобилни телефон, и све остале личне ствари запосленог су преузете, што из стана оптуженог, што из канцеларије у којој је радио. Сада их је неопходно анализирати. Приступа се обради мобилног телефона оптуженог. Сумња се да је лице све украдене податке чувао у вом телефону мислећи да ће ту бити непримећени. Анализом рачунара на радном месту оптуженог није ништа пронађено, сви налози за пренос новца су били правилно одрђени и сумња се никад не би довела на то радно место.



Слика 25. LG Optimus L9

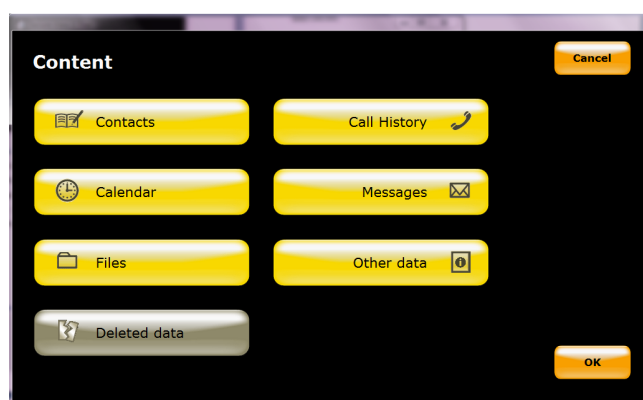
Приступа се обради мобилног телефона оптуженог. У питању је мобилни телефон марке **LG**, модел **Optimus L9** са **IMEI** бројем 353648054072037. Форензичка обрада мобилног телефона ће се вршити помоћу програма **Secure View 3 – Susteen Mobile Forensics**, чија је ужа специјалност прикупљање доказа са мобилних уређаја овог типа.

11.1. Форензичка анализа мобилног телефона



Слика 26. Почетни екран програма

Бирамо опцију **ACQUIRE** да започнемо процес прикупљања података са мобилног телефона и за почетак бирамо опцију **PHONE**, да би приступили меморији телефона и прво одатле прикупили податке. Након тога бирамо опцију да пронађемо телефон који анализирамо, бирамо модел и добијамо форму која нас пита коју врсту података желимо да прикупимо.



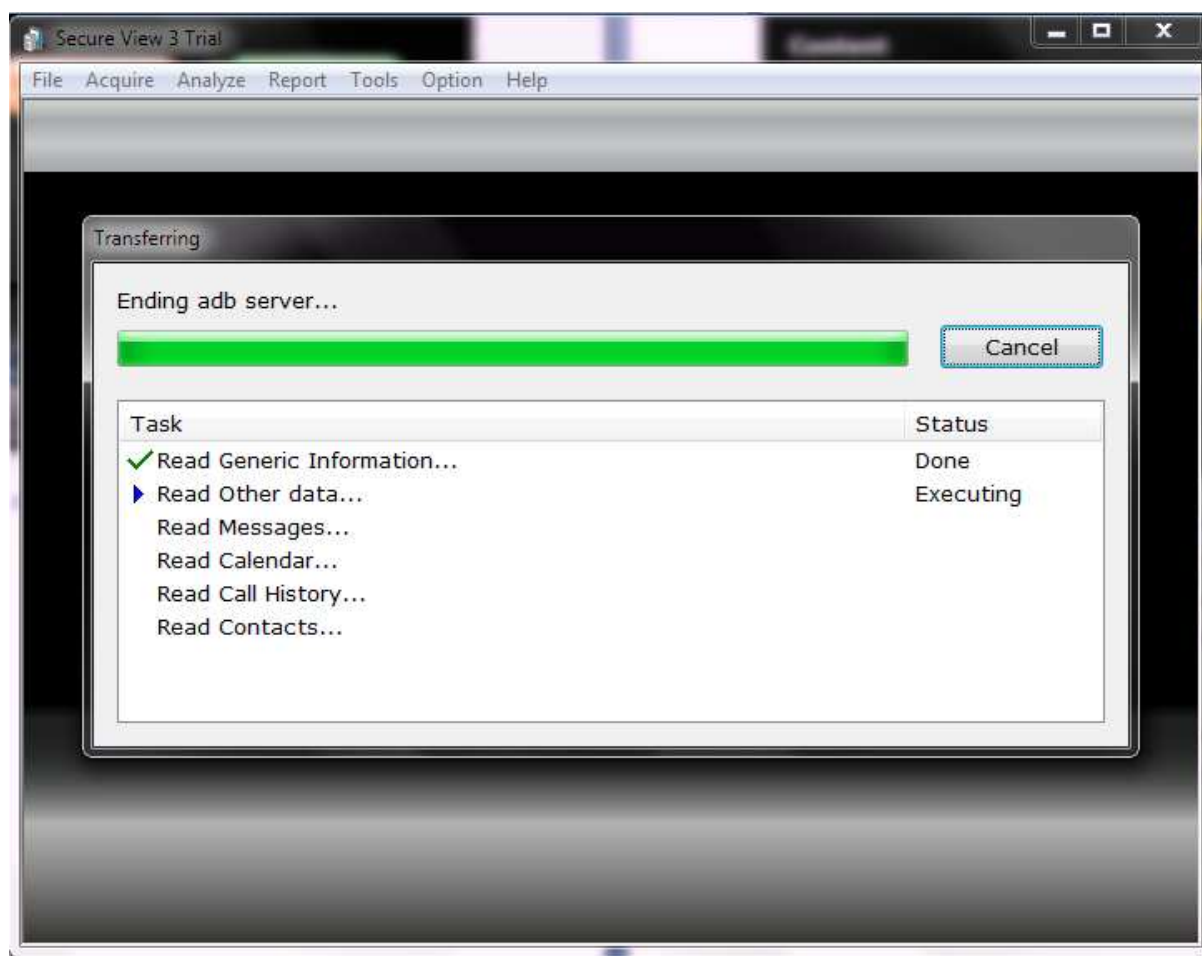
Слика 27. Врста података

Прикупићемо све податке из телефона јер се сумња да се украдени подаци налазе баш ту. Након тога ће се, уколико анализа не пронађе никакве круцијалне податке, прећи на прикупљање других врста података директно са SIM картице.

Након одабраних опција идемо на физичко повезивање телефона са рачунаром. Пре свега је потребно на телефону подесити:

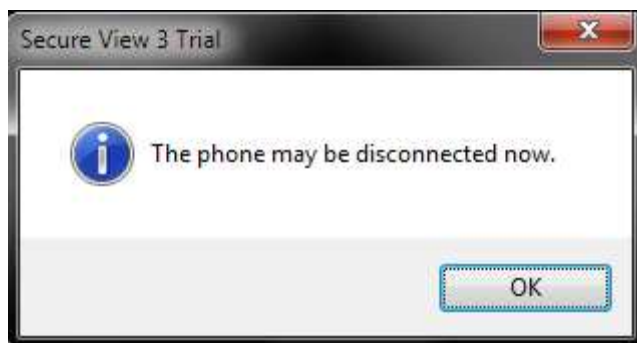
- потребно је у **Settings -> Developer Tools** укључити опцију **USB debugging** који ће нам омогућити несметан приступ свим фајловима телефона без потребних привилегија.

Настављамо даље и програм почиње скенирање и прикупљање података са телефона.



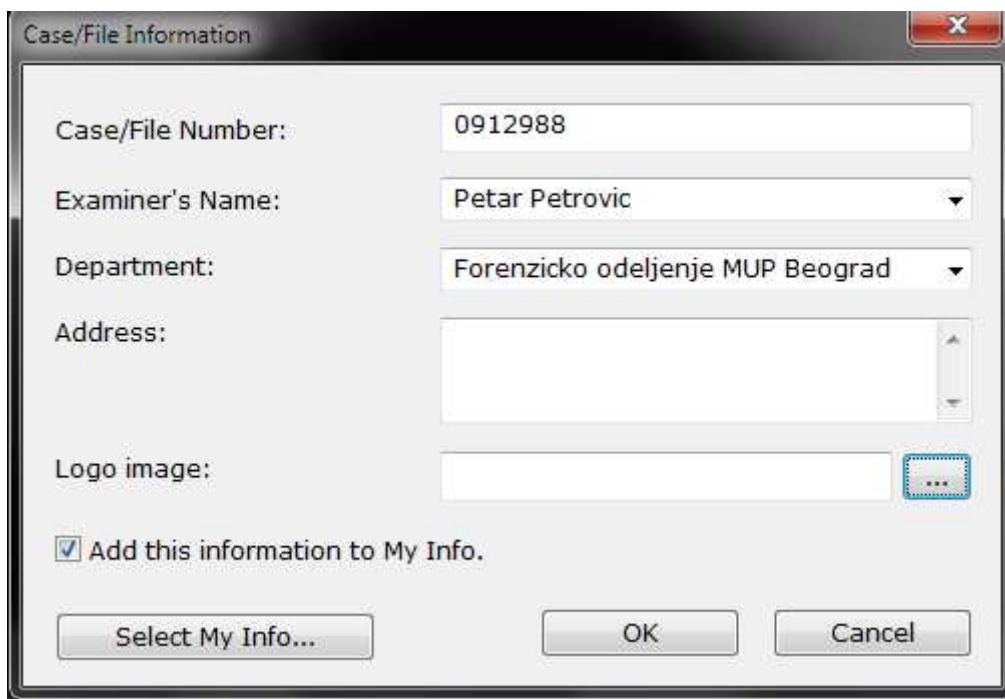
Слика 28. Прикупљање података

Када добијемо следећу поруку значи да је програм завршио читање фајлова са телефона и да можемо приступити прегледу прикупљених информација.



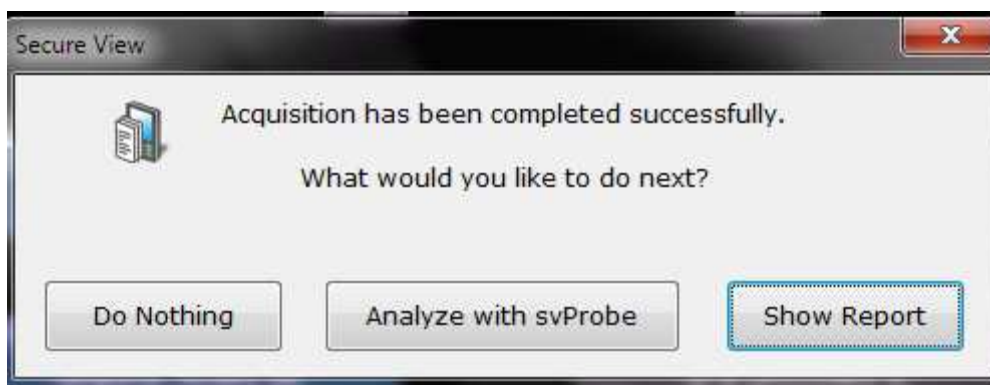
Слика 29. Завршетак процеса прикупљања података

Сада можемо да дефинишемо неке податке за идентификацију овог прикупљања података, фајлови пронађени на телефону сада постају докази и потребно их је тако и завести у рачунару.



Слика 30. Дефинисање истраге

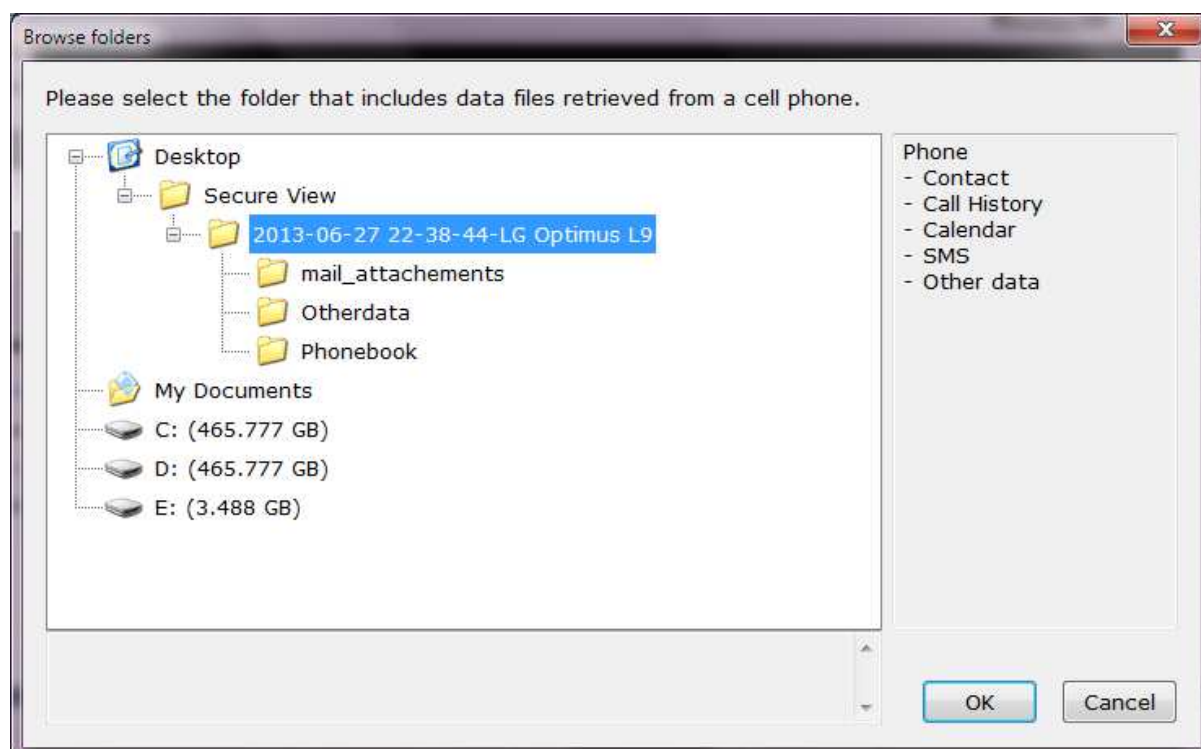
Прелазимо на анализу прикупљених података помоћу додатка програму **svProbe**.



Слика 31. Прелазак на анализу

***НАПОМЕНА:** Нажалост, реална анализа није могућа јер је у питању пробна верзија програма која не дозвољава додавање нове анализе у постојеће примере случајева и доказа.

Додаје се нови извештај. Бирамо фолдер где се налазе преузети фајлови и креирамо нови извештај.



Слика 32. Креирање извештаја

Добијамо извештај и можемо да одаберемо неку од опција: штампа, чување у *pdf* формату, додавање података итд.

Review

>> XML Convert Hash Check Add Data PDF Output Comment Print Close

Summary Activity Trail Contacts Call History Messages Calendar Other data

Secure View 3 (Ver. 3.12.0T)

Case/File Number	0912988
Examiner's Name	Petar Petrovic
Department	Forenzičko odeljenje MUP Beograd

Greenwich Mean Time

Start	06/27/2013 20:38:16
End	06/27/2013 20:54:18

Central Europe Daylight Time

Start	06/27/2013 22:38:16
End	06/27/2013 22:54:18

Country	US
Phone Make	LG
Phone Model	Optimus L9
Phone Number	(entered by examiner)
ESN/IMEI/MEID	353648054072037 (IMEI)
MSI	220011008542646
Security Code	
Wireless Carrier	Telenor
Source Device	Phone / Cable

Након подробне анализе извештаја дошло се до занимљивог податка који је у потпуности доказао кривицу оптуженог лица. Наиме, пронађена је веома чудна смс порука послата дотичној особи Маји Млађеновић.

Review

C:\Users\A6\Desktop\Secure View\2013-06-27 23:33-24-LG Optimus L9

<< Close

Summary Activity Trail Contacts Call History Messages Calendar Other data

No.	817
Date & Time	06/27/2013 23:32:08
To	060 5561878
Name	Maja Mladenović **
Message	janko jankovic janko4.76ja fuuz74j4jv 160-63689479-78 marko stevic marko7.78ste 56zuv 86ihc 160-73358964 99 milos petkovicmilos6.99pet duic688dji 160-25896489-22 maja ml adenovic maja4.87mlade kshdi628ja 160-62949164-77 dobra ivic dobra4.88ivic j4igaj47j u 160-66294629-88 ivica savic ivica2.41savic jape418hso 160-49263928-44 jovana ilic jo vana8.37ilic snd829r62i 160-38492638-22 dragana kolarov dragana5.43kolajaz418gr73 16 0-39592638-29 jelena petrovicjelena6.01pet jakd385vsi 160-37492649-88 stana cigoja stan a5.88cigo h28vs38vv3 160-38495828 98
Status	Sent
Type	SMS

Calendar

MD5: 427bf324587ecfb257e1233c9d7d23bb
SHA1: 4800eeb8325b71e217ca405d0ca0ddfd260e5736

No.	Begin Date & Time	End Date & Time	Title
001	03/12/1970 00:00	03/13/1970 00:00	Rade Pobulić's birthday
002	08/29/1970 00:00	08/30/1970 00:00	Ana Stević's birthday
003	09/22/1970 00:00	09/23/1970 00:00	Milos Petkovic's birthday
004	10/15/1970 00:00	10/16/1970 00:00	Bojana Dimitrijević's birthday
005	11/15/1970 00:00	11/16/1970 00:00	Igor Milenkovic's birthday
006	12/09/1970 00:00	12/10/1970 00:00	Maja Mladenović's birthday

Слика 33. СМС порука

Након анализе дошло се до закључка да су у питању лични приступни подаци клијената наведеног оптуженог лица.

ЕПИЛОГ: Прикупљени подаци су приложени као доказ на суђењу Јовану Слобеновићу. Дотична Маја Млађеновић је приведена при сумњи да је саучесник у злочину и доказано је да је она власник рачуна давно угашене фирме на који је новац пребачен. Оба лица су добила казну од по 5 година затвора а новац је враћен власницима.

12. Закључак

Како се све више ИТ технологија развија и дигитални злочини се све више развијају. Постоји сваког дана све више начина за преваре и разне злочине путем рачунара. Велика већина злочина који се одвијају уживо могу се чинити и путем рачунара или интернета.

Електронски доказ има све већи значај и због тога се са њима мора поступати врло пажљиво. Често се прикупљање и анализа тих доказа не може обавити помоћу једног алата већ комбинацијом више њих. Сваки од алата је намењен једној или више фаза истраге. Често су дигитални трагови оштећени, под заштитом или изгубљени или избрисани, због тога се морају користити различити алати.

Главни недостатак свих алата је то што је велика већина њих лиценцирана и цене лиценци су веома високе, што наравно зависи од тога какве су намене тог програма и колико могућности пружају и да ли је могуће докупљивати његове додатке.

Иако су алати скупи њихова примена је од кључног значаја за форензичку истрагу и због тога је њихова употреба оправдана.

Циљ је да се скрене пажња на изузетно рањиве мале системе "паметних" уређаја који су са нама сваког дана а нисмо свесни опасности које из њих вребају и у које можемо доћи уколико се неко дочепа података са тих уређаја. Ти исти уређаји могу нас заштитити уколико је потребно. Сви ови мобилни уређаји на овај или онај начин могу бити доказни материјал против неког злочинца. Важно је употребити га на прави начин.

У последњих неколико година законске одредбе су се мењале да би подаци прикупљени са мобилних уређаја били признати на суду уколико прођу верификацију и валидацију. Мобини уређаји су део свакодневнице, сваки човек је део свога дана спојен са барем једним таквим уређајем, ако не и са више. Посебно је изазов и јако добра мета злонамерних то што су мобилни уређаји

све "паметнији" и све више података о нама самима садрже у себи, почев од личних ствари па све до пословних, које су управо мета криминалаца.

13. Литература

- [1.] Anthony Reyes, Jack Wiles, *The Best Damn Cybercrime and Digital Forensics book Period*, 2007.
- [2.] Семинар о *Cyber* тероризму – *Кризе и кризно управљање*, Хрватска, 27.03.2012.
- [3.] *Конвенција о високотехнолошком криминалу*, Будимпешта, 23.11.2001.
- [4.] Службени гласник РС, *Кривични законик Републике Србије*, бр.85/05, 88/05 и 107/05.
- [5.] Службени гласник РС, *Закон о посебним овлашћењима ради заштите права интелектуалне својине*, број 46/06.
- [6.] Access Data, *FTK Manual*, 2003.
- [7.] Хрватска академска и истраживачка мрежа, *Рачунална форензика*, 2010.
- [8.] Yong Wang, Kevin Streff, Sonell Raman, *Smartphone Security Challenges*, 2012.
- [9.] Casey, E., *Digital evidence and computer crime: forensic science, computers, and the Internet*, 2004.
- [10.] Willassen S., *Forensic analysis of mobile phone internal memory*, 2005.
- [11.] Keonwoo Kim, Dowon Hong, Kyoil Chung, Jae-Cheol Ryou, *Data Acquisition from Cell Phone using Logical Approach*, 2007.
- [12.] Mokhonoana P., Olivier M., *Acquisition of a Symbian smart phone's content with an on-phone forensic tool*, 2007.
- [13.] <http://www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-osnove.htm> (посећено 24.03.2013.)
- [14.] www.vreme.com, *Српска форензика: Отисак прста, чаура, ДНК*, 12.01.2012. (посећено 03.03.2013.)
- [15.] http://en.wikipedia.org/wiki/Digital_forensics (посећено 01.03.2013.)
- [16.] <http://beograd.vtk.jt.rs/> (посећено 15.03.2013.)
- [17.] http://sh.wikipedia.org/wiki/Mobilni_telefon (04.05.2013.)
- [18.] http://sr.wikipedia.org/sr/USB_memorija (04.05.2013.)
- [19.] http://www.trustedreviews.com/opinions/how-it-works-memory-cards_Page-3 (17.05.2013.)
- [20.] <http://stevelitchfield.com/historyofpsion.htm> (14.05.2013.)

- [21.] <http://saveti.kombib.rs/sigurnost-podataka-na-usb-flash-memoriji.html>
(14.05.2013.)
- [22.] <http://www.advansysperu.com/usb-lock-standard.html> (17.05.2013.)
- [23.] <http://www.datasolutions.rs/srp/spasavanje-podataka/spasavanje-podataka-sa-digitalnih-medija.html> (25.05.2013.)
- [24.] <http://igorfranc.blogspot.com/2012/11/digitalna-forenzika-mobilnih-telefona-i.html> (29.05.2013.)
- [25.] http://en.wikipedia.org/wiki/Boundary_scan
- [26.] http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic:_digitalna_forenzika_mobilnih_telefona_za_potrebe_krivicnog_postupka.377.html (06.05.2013.)
- [27.] <https://viaforensics.com/resources/white-papers/iphone-forensics/micro-systemation-xry/#forensic-acquisition> (10.06.2013.)
- [28.] http://en.wikipedia.org/wiki/Digital_forensics
- [29.] http://sr.wikipedia.org/sr/digitalna_forenzika_i_alati
- [30.] http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf
- [31.] http://www.dataprotection2003.info/speakers/Marijan_Risteski/presentation.pdf
- [32.] <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>
- [33.] <http://www.infoteh.rs.ba/rad/2012/RSS-4/RSS-4-9.pdf>
- [34.] <http://ad-pdf.s3.amazonaws.com/ImagerUsersGuide.pdf>